NOTAS DE TRABAJO, 6

ÁLGEBRA CONMUTATIVA

Pascual Jara Martínez

Departamento de Álgebra. Universidad de Granada

Granada, 1997–2012

Primera redacción: 1997.
Segunda redacción: Octubre 2007.
Tercera redacción: Octubre 2008.
Cuarta redacción: Octubre 2009.
Quinta redacción: Agosto 2011.
Sexta redacción: Septiembre 2012.

Introduction

Este texto de Álgebra Conmutativa Básica es la continuación natural del de Álgebra Conmutativa Elemental. Mientras que en el primero exponíamos los rudimentos de la aritmética de los enteros y de los polinomios en una variable, y por ende de los Dominios de Ideales Principales, acabando con el estudio de la estructura de los módulos finitamente generados sobre un DIP, la intención primera de este texto es el estudio de los anillos de polinomios en varias indeterminadas con coeficientes en un cuerpo.

Haremos un uso extensivo de las técnicas de computación que nos proporciona la división en estos anillos, lo que nos conducirá a la introducción de las bases de Groebner. Con esta herramienta estudiaremos las propiedades de los ideales sobre anillos de polinomios.

Para el estudio de los conjuntos de puntos asociados a ideales, y obtener una buena relación entre ideales radicales y conjuntos algebraicos necesitaremos que el cuerpo base sea algebraicamente cerrado: Teorema de los ceros de Hilbert. Probamos este resultado estableciendo previamente el Lema de normalización de Noether. Esta teoría se completa con el estudio de las cadenas de ideales primos y la noción de dimensión de Krull.

De forma paralela, y un tanto marginal, introducimos los módulos sobre un anillo y caracterizamos éste mediante propiedades elementales de sus módulos.

Índice general

Parte I

Álgebra Conmutativa Básica

Introducción

Este texto recoge las nociones básicas de Álgebra Conmutativa y los rudimentos de Geometría Algebraica. Desde el primer momento en él hacemos hincapié en el maridaje existente entre nociones abstractas y nociones computacionales, tratando de profundizar en cada una de ellas, y centrándonos en el cálculo efectivo de los invariantes que vamos introduciendo.

En cada capítulo hacemos primero un desarrollo de la teoría procurando incluir en el mismo un gran número de ejemplos que ilustren los conceptos introducidos, y lo cerramos con una sección dedicada a ejercicios; la gran mayoría de los cuales se exponen acompañados de una solución, que aparece en la última sección del capítulo.

Capítulo I

Anillos e ideales

Introducción

En este capítulo se introducen, entre otros, los conceptos de anillo y homomorfismo de anillos; y en particular aquellos que tienen relación con los ideales,

Los anillos objeto de este estudio son anillos conmutativos abstractos, por lo que los ideales estudiados son ideales biláteros. Esto hace especialmente sencillo el estudio de su estructura a través de los ideales primos y maximales y los correspondientes radicales: el nilradical y el radical de Jacobson.

Se extiende el radical de un anillo al radical de un ideal utilizando la correspondencia biyectiva, para cada homomorfismo $f : A \longrightarrow B$, entre los ideales de $\operatorname{Im}(f)$ y los ideales de A que contienen a $\operatorname{Ker}(f)$. En particular se estudian la extensión y la contracción de ideales para un homomorfismo de anillos.

El capítulo concluye con una sección dedicada a las álgebras sobre un anillo; introducimos los anillos de series formales y nos centramos especialmente en las álgebras finitamente generadas y los anillos de polinomios.

1. Definición de anillo

Un **anillo** [1] es un grupo abeliano $(A,+)$ junto con una operación binaria

$$\times : A \times A \longrightarrow A,$$

llamada **producto** o **multiplicación**, verificando las siguientes propiedades:

(A-I) Es **asociativa**, esto es; para cualesquiera a, b, $c \in A$ se tiene $a \times (b \times c) = (a \times b) \times c$.

(A-II) Tiene **elemento uno**, esto es; existe un elemento $1 \in A$ tal que para cualquier elemento $a \in A$ se tiene $a \times 1 = a = 1 \times a$.

(A-III) El producto es **distributivo** respecto a la suma, esto es; para cualesquiera a, b, $c \in A$ se tiene $a \times (b+c) = (a \times b) + (a \times c)$ y $(b+c) \times a = (b \times a) + (c \times a)$.

Ejemplos. 1.1.
Hay dos ejemplos arquetípicos de anillo; uno es el anillo $\mathbb{Z}$ de los números enteros, y otro es el que proporciona el anillo $\mathrm{End}(M)$ de los endomorfismos de un grupo abeliano M, en el que la suma está definida punto a punto, la multiplicación es la composición y el uno es la identidad.

Si además el producto verifica la propiedad:

(A-IV) **Conmutativa**, esto es; para cualesquiera $a, b \in A$ se tiene $a \times b = b \times a$;

entonces el anillo se llama un **anillo conmutativo**.

Dado un elemento a de un anillo $(A,+,\times,1)$, un **elemento inverso** de a es un elemento $b \in A$ tal que $a \times b = 1 = b \times a$. Un elemento $a \in A$ que tiene inverso se dice que es **invertible** o también que es una **unidad**.

Un anillo A en el que todo elemento no nulo tiene un inverso decimos que es un **anillo de división**. Un anillo de división conmutativo se llama un **cuerpo**.

[1] El nombre de *anillo* (*ring* en inglés) es debido a David Hilbert (Königsberg-1862, Göttingen-1943). La historia que conduce a la introducción de la estructura abstracta de anillo tiene su punto culminante en 1888, cuando Hilbert, a la edad de 26 años, asombra a la comunidad matemática resolviendo el "*problema de Gordan*". Veinte años antes Paul Gordan (Breslau-1837, Erlander-1912) prueba que *las formas binarias tienen una base finita*, y se plantea el mismo problema para formas ternarias, ... La demostración dada por Gordan era larga y complicada y no susceptible de aplicación para la resolución del problema. La solución que presenta Hilbert es elegante y novedosa y además supone un cambio en el paradigma de la resolución de problemas en Matemáticas.
Primero introduce el concepto de *Zahlring* (*anillo de números*), que engloba al los anillos de números: enteros, racionales, reales, etc. y los ejemplos *nuevos*: polinomios sobre éstos. Los anillos son la estructura que recoge las propiedades de estos conjuntos y las operaciones suma, producto y uno.
Segundo establece que sin un anillo R verifica la propiedad de que todo *ideal*, introducido por R. Dedekind (Braunschweig-1831,1916), es finitamente generado, esta propiedad también es cierta para el anillo de polinomios $R[X]$, y posteriormente extiende este resultado a anillos $R[X_1][X_2]\ldots[X_n]$.
A diferencia de la prueba de Gordan, establece que si un ideal de $R[X]$ no fuese finitamente generado, se llegaría a una contradicción; pero no da una construcción explícita de base alguna. Este es el punto esencial para el desarrollo de la Matemática, ya que establece que no es necesario utilizar métodos constructivos.
Son claras las ventajas de este nuevo método (de reducción al absurdo o de contradicción) para construir la Matemática. Sin embargo esto no fue así advertido en un principio, pues el mismo Gordan decía: "*Das ist nicht Mathematik, das ist Theologie*". Aunque finalmente reconoce que *también la Teología tiene ventajas para el desarrollo de la Matemática*, después de que Hilbert en 1892 da una prueba constructiva para el problema de Gordan.

Lema. 1.2.
El conjunto $A^{\times}$ de los elementos invertibles de un anillo A, junto con la multiplicación, es un grupo (abeliano si A es conmutativo).

En este texto vamos a trabajar con anillos conmutativos, a los que designaremos simplemente como *anillos*. Para cualesquiera elementos $a, b \in A$ el elemento $a \times b$ lo representaremos por ab y lo llamaremos el *producto* ó *multiplicación* de a por b.

Los siguientes resultados son obvios a partir de las definiciones anteriores, y puede decirse que constituyen la base de la aritmética de los anillos (conmutativos).

Lema. 1.3.
Sea A un anillo, los siguientes enunciados son ciertos:

(1) Los elementos cero y uno están determinados de forma única;
(2) Para cada elemento $a \in A$ el opuesto y el inverso, si éste último existe, están determinados de forma única.

DEMOSTRACIÓN. (1). Si x e y son ceros de A, entonces $x = x + y = y$.
Si x e y son unos de A, entonces $x = xy = y$.
(2). Si x e y son opuestos de $a \in A$, entonces $x = x + 0 = x + (a + y) = (x + a) + y = 0 + y = y$.
Si x e y son inversos de $a \in A$, entonces $x = x1 = x(ay) = (xa)y = 1y = y$. □

El **elemento cero** se representa por 0, y el **elemento uno** se representa por 1. El **opuesto** de un elemento $a \in A$ se representa por $-a$, y si $a \neq 0$, el **elemento inverso** de a, si existe, se representa por a^{-1}.

Proposición. 1.4.
Sea A un anillo, se verifica:

(1) $a0 = 0$ para todo $a \in A$.
(2) A tiene más de un elemento si, y sólo si, $0 \neq 1$.
(3) $(-a)b = -(ab) = a(-b)$, para todos $a, b \in A$. En particular $(-1)a = -a$.
(4) $(n \cdot a)b = n \cdot (ab) = a(n \cdot b)$, para todos $a, b \in A$ y $n \in \mathbb{Z}$.
(5) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$, para todos $a_i, b_j \in A$ y $n, m \in \mathbb{N}^*$.
*(6) **Fórmula de Newton.** $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$, para todos $a, b \in A$ y $n \in \mathbb{N}$.*
(7) $(ab)^n = a^n b^n$ y $(a^n)^m = a^{nm}$, para todos $a, b \in A$ y $n, m \in \mathbb{Z}$.

DEMOSTRACIÓN. (1). Para cada $a \in A$ se tiene $a = a1 = a(1 + 0) = a1 + a0 = a + a0$, luego $a0 = 0$.

(2). Si $0 \neq 1$ en A, entonces A tiene más de un elemento. Si $0 = 1$, entonces para cada $a \in A$ se tiene $a = a1 = a0 = 0$.

(3). Para $a, b \in A$ se tiene $0 = a0 = a(b - b) = ab + a(-b)$, luego $a(-b) = -(ab)$. Y de la misma forma $(-a)b = -(ab)$.

(4). Para $n \geq 0$ se hace por inducción sobre n. Si $n < 0$, entonces $0 = 0a = (n - n)a = na + (-n)a$, luego $(-n)a = -(na)$, lo que permite completar el resultado.

(5). Por inducción sobre n y m.

(6). Por inducción sobre n.

(7). Por inducción sobre n y m. □

Corolario. 1.5.
Sea A un anillo, para $a, b \in A$ y para $n, m \in \mathbb{Z}$ se verifica:

$$(n \cdot a)(m \cdot b) = (nm) \cdot (ab).$$

Según hemos visto, cuando el elemento 1 coincide con el elemento 0, entonces todos los elementos del anillo son iguales. Estos anillos se llaman **anillos triviales**. Los anillos que vamos a considerar son, en general, anillos no triviales.

Observación. 1.6.
Observar que la existencia de elemento uno forma parte de la definición de anillo. Así el conjunto $2\mathbb{Z}$, junto con la suma y el producto usuales, no es un anillo, ya que no tiene elemento uno.

2. Homomorfismos de anillos

Sean A y B anillos, una aplicación $f : A \longrightarrow B$ se llama un **homomorfismo de anillos** si verifica las siguientes propiedades:

(HA-I) Para cualesquiera $a, b \in A$ se tiene $f(a+b) = f(a) + f(b)$.
(HA-II) Para cualesquiera $a, b \in A$ se tiene $f(ab) = f(a)f(b)$.
(HA-III) $f(1) = 1$.

Proposición. 2.1.
Para cada anillo A existe un único homomorfismo de anillos $f : \mathbb{Z} \longrightarrow A$.

Proposición. 2.2.
Si $f : A \longrightarrow B$ y $g : B \longrightarrow C$ son homomorfismos de anillos, entonces la composición $g \circ f : A \longrightarrow C$ es un homomorfismo de anillos.
La composición de homomorfismos de anillos es asociativa.

Proposición. 2.3.
Para cada anillo A existe un homomorfismo $\mathrm{id}_A : A \to A$ definido $\mathrm{id}_A(a) = a$ para cada elemento $a \in A$; este homomorfismo verifica:
(1) Para cada homomorfismo $f : A \to B$ se tiene $f \circ \mathrm{id}_A = f$ y
(2) Para cada homomorfismo $g : C \to A$ se tiene $\mathrm{id}_A \circ g = g$.

Subanillos

Si $f : A \longrightarrow B$ un homomorfismo de anillos el subconjunto

$$\mathrm{Im}(f) = \{f(a) \in B \mid \ a \in A\}$$

de B verifica las siguientes propiedades:

(SA-I) Es un subgrupo de B.
(SA-II) Es cerrado para la multiplicación en B.
(SA-III) $1 \in \mathrm{Im}(f)$.

En general un subconjunto A' de un anillo A verificando las propiedades (SA-I), (SA-II) y (SA-III) se llama un **subanillo** de A.
El conjunto de los subanillos de un anillo A verifica algunas propiedades de interés. Entre ellas destacamos la siguiente:

Lema. 2.4.
Si $\{A_\alpha \mid \alpha \in \Gamma\}$ *es una familia de subanillos de A, entonces también lo es su intersección* $\cap_\alpha A_\alpha$.

Como consecuencia, dado un subconjunto $\mathcal{X}$ de A podemos considerar el menor subanillo de A que contiene a $\mathcal{X}$, éste es simplemente la intersección

$$\cap\{B \mid \mathcal{X} \subseteq B, \text{ y } B \text{ es un subanillo de } A\}.$$

Se llama el **subanillo generado** por $\mathcal{X}$.

Ejercicio. 2.5.
Prueba que los elementos del subanillo generado por $\mathcal{X}$ *son las expresiones polinómicas en elementos de* $\mathcal{X} \cup \{1\}$ *con coeficientes en* $\mathbb{Z}$.

Este subanillo generado por $\mathcal{X}$ se representa por $\langle \mathcal{X} \cup \{1\} \rangle$.

Ideales

Por otro lado, dado un homomorfismo de anillos $f : A \longrightarrow B$, el subconjunto de A

$$\operatorname{Ker}(f) = \{x \in A \mid f(x) = 0\}$$

verifica las siguientes propiedades:
(ID-I) Es un subgrupo de A;
(ID-II) Para cualesquiera $a \in A$ y $x \in \operatorname{Ker}(f)$ se tiene $ax \in \operatorname{Ker}(f)$.

En general definimos un **ideal** de un anillo A como un subconjunto $\mathfrak{a}$ de A verificando las propiedades (ID-I) y (ID-II). Un ideal $\mathfrak{a}$ de A es **propio** si $\mathfrak{a} \neq A$, y **no trivial** si $\mathfrak{a} \neq \{0\}$.
Los ideales verifican algunas propiedades interesantes. Por ejemplo:

Lema. 2.6.
*(1) La **intersección** de una familia de ideales* $\{\mathfrak{a}_\alpha \mid \alpha \in \Gamma\}$ *es un ideal y*
*(2) la **suma** de una familia de ideales,* $\{\mathfrak{a}_\alpha \mid \alpha \in \Gamma\}$*, definida como,*

$$\sum\{\mathfrak{a}_\alpha \mid \alpha \in \Gamma\} = \left\{\sum a_{\alpha_j} \mid \alpha_j \in F \subseteq \Gamma \text{ finito, } a_{\alpha_j} \in \mathfrak{a}_{\alpha_j}, \text{ para todo } \alpha_j \in F\right\}$$

es un ideal.

Decimos que el ideal $\mathfrak{a}$ es **menor** que el ideal $\mathfrak{b}$ si $\mathfrak{a} \subseteq \mathfrak{b}$. Esto define una relación de orden, $\mathfrak{a} \leq \mathfrak{b}$, en el conjunto, $\mathcal{L}(A)$, de todos los ideales del anillo A. Respecto a este orden el **ínfimo** de una familia de ideales es la intersección y el **supremo** es la suma.

Dado un subconjunto $\mathcal{X}$ de A, existe un menor ideal, representado por $A\mathcal{X}$ ó $(\mathcal{X})$, que contiene a $\mathcal{X}$, y que se puede definir como la intersección de todos los ideales de A que contienen a $\mathcal{X}$. Se llama el **ideal generado** por $\mathcal{X}$ y el conjunto $\mathcal{X}$ se dice que es un **sistema de generadores** de $A\mathcal{X}$.

Ejercicio. 2.7.
Prueba que los elementos de $A\mathcal{X}$ son todas las expresiones (finitas) de la forma $\sum_i a_i x_i$, con $a_i \in A$ y $x_i \in \mathcal{X}$.

En el caso en el que $\mathcal{X} = \{x\}$, la descripción de $(\mathcal{X})$ es especialmente sencilla:

$$(\mathcal{X}) = (x) = \{ax \mid \; a \in A\} = Ax.$$

Llamaremos a $(x) = Ax$ el **ideal principal** generado por x.

Un ideal $\mathfrak{a}$ de A se llama **finitamente generado** si existe un subconjunto finito $\mathcal{X}$ de A tal que $\mathfrak{a} = (\mathcal{X})$.

Existe otra operación entre ideales, el **producto de ideales**, definido de la siguiente forma: sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un anillo A, definimos $\mathfrak{ab}$ como el conjunto de todas las expresiones finitas de la forma $\sum\{a_i b_i \mid \; a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$. Es claro que $\mathfrak{ab}$ es el ideal generado por los productos ab con $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ y está contenido en la intersección de $\mathfrak{a}$ y $\mathfrak{b}$.

Dados dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ se define un nuevo ideal, el **ideal residual** de $\mathfrak{a}$ por $\mathfrak{b}$

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid \; x\mathfrak{b} \subseteq \mathfrak{a}\}.$$

Lema. 2.8.
Para cada dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ se tiene que $(\mathfrak{a} : \mathfrak{b})$ es un ideal que contiene a $\mathfrak{a}$.

Anillo cociente

Sea $\mathfrak{a}$ un ideal de un anillo A. En el grupo cociente $A/\mathfrak{a}$ podemos definir una operación binaria mediante:

$$(a + \mathfrak{a})(b + \mathfrak{a}) = ab + \mathfrak{a},$$

con esta operación $A/\mathfrak{a}$ tiene estructura de anillo, con elemento uno igual a $1+\mathfrak{a}$, y la aplicación canónica

$$p : A \longrightarrow A/\mathfrak{a}$$

es un homomorfismo de anillos. El anillo $A/\mathfrak{a}$ se llama el **anillo cociente** de A por el ideal $\mathfrak{a}$.

Este proceso de la construcción del anillo cociente está determinado de forma única en el siguiente sentido. Sea A un anillo, una relación de equivalencia $\sim$ se llama **compatible** con las operaciones de A si verifica:

$$\begin{array}{l}\text{si } a \sim b \text{ y } a' \sim b', \text{ entonces } a+b \sim a'+b', \\ \text{si } a \sim b \text{ y } a' \sim b', \text{ entonces } ab \sim a'b'.\end{array}$$

Es claro que si $\sim$ es una relación de equivalencia en un anillo A, entonces $\sim$ es compatible si, y sólo si, en $A/\sim$ podemos definir una estructura de anillo mediante:

$$\begin{array}{l}[a]+[b]=[a+b], \\ [a]\times[b]=[a\times b],\end{array}$$

y donde el elemento uno es $[1]$. Esto es, tal que la proyección $p : A \longrightarrow A/\sim$ sea un homomorfismo de anillos.

Además una relación de equivalencia compatible $\sim$ determina un ideal $\mathfrak{a}$ de A en la siguiente forma:

$$\mathfrak{a} = \{a \in A \mid \ a \sim 0\},$$

y recíprocamente, dado un ideal $\mathfrak{a}$ de A, la relación $\sim$ definida por $a \sim b$ si $a-b \in \mathfrak{a}$ es una relación de equivalencia compatible.

Proposición. 2.9.
Para cada anillo A existe una correspondencia biyectiva entre:

(I) *relaciones de equivalencia compatibles en A,*
(II) *ideales de A.*

Propiedad universal del anillo cociente

Proposición. 2.10. (Propiedad universal del anillo cociente)
Dado un anillo A y un ideal $\mathfrak{a} \subseteq A$, para cada homomorfismo de anillos $f : A \longrightarrow B$ tal que $f(\mathfrak{a}) = 0$ existe un único homomorfismo de anillos $f' : A/\mathfrak{a} \longrightarrow B$ tal que $f = f' \circ p$. Esto es, el siguiente diagrama conmuta.

$$\begin{array}{ccc} A & \xrightarrow{p} & A/\mathfrak{a} \\ & {}_{f}\searrow & \swarrow_{\exists_1 f'} \\ & B & \end{array}$$

Un homomorfismo de anillos $f : A \longrightarrow B$ es un **isomorfismo** si existe un homomorfismo de anillos $g : B \longrightarrow A$ tal que $f \circ g = \mathrm{id}_B$ y $g \circ f = \mathrm{id}_A$, o equivalentemente si f es una aplicación inyectiva y sobreyectiva, esto es, una biyección.

Proposición. 2.11. (Primer Teorema de Isomorfía)
Dado un homomorfismo de anillos $f : A \longrightarrow B$, existe un único homomorfismo natural f' que completa el siguiente diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ A/\operatorname{Ker}(f) & \underset{\exists_1 f'}{\dashrightarrow} & \operatorname{Im}(f) \end{array}$$

Además f' es un isomorfismo.

Proposición. 2.12.
La imagen del único homomorfismo $f : \mathbb{Z} \longrightarrow A$ se llama el ***subanillo característico*** *de A.*
El núcleo de f es un ideal de $\mathbb{Z}$, por lo tanto es de la forma $n\mathbb{Z}$, para $n \geq 0$. Llamamos a n la ***característica*** *del anillo A.*

Ejemplo. 2.13.
Para cada ideal $n\mathbb{Z}$ el anillo $\mathbb{Z}/n\mathbb{Z}$ se representa por $\mathbb{Z}_n$, y está formado por las clases de $\mathbb{Z}$ módulo n. Como consecuencia del Primer Teorema de Isomorfía, si A tiene característica $n > 0$, entonces contiene un subanillo isomorfo a $\mathbb{Z}_n$; y si tiene característica cero, entonces contiene un subanillo isomorfo a $\mathbb{Z}$.

3. Producto de anillos

Producto de anillos

Dada una familia de anillos $\{A_i \mid i \in I\}$, en el producto cartesiano $\prod_i A_i$ consideramos dos operaciones definidas componente a componente

$$\begin{array}{l} (a_i)_i + (b_i)_i = (a_i + b_i)_i, \\ (a_i)_i \times (b_i)_i = (a_i \times b_i)_i, \end{array}$$

que junto con el elemento $1 = (e_i)_i$, siendo $e_i \in A_i$ el elemento uno, verifican:

Lema. 3.1.
Con la notación anterior $(\prod_i A_i, +, \times, 1)$ *es un anillo, que es conmutativo si, y solo si, cada* A_i *es conmutativo.*

Para cada índice $j \in I$ definimos:

$$\begin{array}{ll} \alpha_j : A_j \to \prod_i A_i, & \alpha_j(x) = (x\delta_{i,j})_i, \text{ siendo } \delta_{i,j} = \begin{cases} e_i \in A_i \text{ si } j = i, \\ 0 \in A_i \text{ si } j \neq i. \end{cases} \\ \beta_j : \prod_i A_i \to A_j, & \beta_j((a_i)_i) = a_j. \end{array}$$

El par $(\prod_{i\in I} A_i, \{\beta_j \mid i \in I\})$ se llama el **anillo producto directo** de la familia $\{A_i \mid i \in I)\}$

Lema. 3.2.
Con la notación anterior se tiene

(1) α_j *es un homomorfismo inyectivo para la suma y el producto, pero* <u>*no*</u> *es un homomorfismo de anillos salvo que* I *sea unitario.*

(2) β_j *es un homomorfismo de anillos.*

(3) $\beta_k \circ \alpha_j = \delta_{j,k}$*, siendo* $\delta_{j,k} = \begin{cases} \mathrm{id}_{A_j}, \text{ si } k = j \\ 0 : A_j \to A_k, \text{ si } k \neq j. \end{cases}$

(4) ***Propiedad universal del anillo producto.*** *Para cada anillo* B *y cada familia de homomorfismo de anillos* $\{f_i : B \to A_i \mid i \in I\}$*, existe un único homomorfismo de anillos* $f : B \to \prod_i A_i$ *tal que* $f_i = \beta_i \circ f$.

$$\begin{array}{ccc} B & & \\ {\scriptstyle \exists_1 f} \downarrow & \searrow^{f_i} & \\ \prod_i A_i & \xrightarrow[\beta_i]{} & A_i \end{array}$$

Lema. 3.3.
Con la notación anterior, si $I = \{1, \ldots, t\}$ es un conjunto finito, se verifica:

(1) $\sum_{j=1}^{t} \alpha_i \circ \beta_i = id_{\prod_i A_i}$.
(2) $\mathrm{Im}(\alpha_i)$ *es un ideal de* $\prod_i A_i$, *y* $\sum_{i=1}^{t} \mathrm{Im}(\alpha_i) = \prod_{i=1}^{t} A_i$.
(3) $\mathrm{Ker}(\beta_j) = \sum_{i \neq j} \mathrm{Im}(\alpha_i)$ *y* $\mathrm{Ker}(\beta_j) \cap \mathrm{Im}(\alpha_j) = 0$.

Lema. 3.4.
Sea A un anillo y $\mathfrak{a}_1, \ldots, \mathfrak{a}_t \subseteq A$ ideales no nulos tales que

(I) $\mathfrak{a}_j \cap \left(\sum_{i \neq j} \mathfrak{a}_i\right) = 0$ *y*
(II) $\sum_{i=1}^{t} \mathfrak{a}_i = A$

Un conjunto de ideales verificando estas condiciones se llama un ***conjunto independiente*** *de ideales de A. Se verifica:*

(1) Existe un isomorfismo, para la suma y el producto, $\prod_{i=1}^{t} \mathfrak{a}_i \cong A$, definido $(a_1, \ldots, a_t) \mapsto a_1 + \cdots + a_t$.
(2) Cada $\mathfrak{a}$ es un anillo con elemento uno e_i tal que $e_1 + \cdots + e_t = 1$; en este caso $\mathfrak{a}_i = e_i A$.
(3) Se tiene $e_i e_j = \delta_{i,j}$. En particular cada e_i es un elemento idempotente.
Un conjunto de elementos $\{e_1, \ldots, e_t\}$ verificando $e_i e_j = \delta_{i,j}$ y $e_1 + \cdots + e_t = 1$ se llama un ***conjunto completo de elementos idempotentes ortogonales*** *del anillo A.*
(4) Si e, f son elementos idempotentes tales que $eA = fA$, entonces $e = f$.
(5) Existe una biyección entre conjuntos completos de idempotentes ortogonales de A y conjuntos independientes de ideales de A.

DEMOSTRACIÓN. (4). Si $eA = fA$, existen $a, b \in A$ tales que $e = fa$ y $f = eb$. Se tiene:

$$e = fa = (eb)a = eab = faab = ffab = fafab = eeb = eb = f.$$

□

Un anillo A se llama **descomponible** si contiene un idempotente $e \in A$ tal que $e \neq 0, 1$, en caso contrario se dice **indescomponible**.

Teorema chino del resto

Dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ de un anillo A se llaman **comaximales** o **primos relativos** si $\mathfrak{a} + \mathfrak{b} = A$.

Lema. 3.5.
Sea A un anillo, si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales comaximales, entonces se verifica: $\mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$.

DEMOSTRACIÓN. Siempre se verifica que $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$. Por otro lado sea $x \in \mathfrak{a} \cap \mathfrak{b}$, por la hipótesis existen $a \in \mathfrak{a}$ y $b \in \mathfrak{b}$ tales que $a + b = 1$, entonces $x = ax + bx \in \mathfrak{a}\mathfrak{b}$, y se verifica la igualdad. □

Proposición. 3.6. (Teorema chino del resto.)
Sean A un anillo, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *ideales de A y f la aplicación canónica definida por las proyecciones* $p_i : A \to A/\mathfrak{a}_i$, $i = 1, \ldots, n$:

$$f : A \longrightarrow \prod_{i=1}^{n} A/\mathfrak{a}_i, \qquad f(a) = (a + \mathfrak{a}_i)_i$$

Entonces se verifica:

(1) Si $\mathfrak{a}_i$ y $\mathfrak{a}_j$ son comaximales, cuando $i \neq j$, entonces $\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$;
(2) f es sobreyectiva si, y sólo si, $\mathfrak{a}_i$ y $\mathfrak{a}_j$ son comaximales si $i \neq j$, para todos los índices i, j;
(3) f es inyectiva si, y sólo si, $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = 0$.

DEMOSTRACIÓN. (1). Hacemos inducción sobre n. Para $n = 2$ es el Lema (3.5.). Supongamos que es cierto para $n-1$; ya que $\mathfrak{a}_i + \mathfrak{a}_n = A$, para $1 \leq i \leq n-1$, tomamos $x_i \in \mathfrak{a}_i$, $y_i \in \mathfrak{a}_n$ tal que $x_i + y_i = 1$. Construimos entonces:

$$x_1 \cdots x_{n-1} = (1 - y_i) \cdots (1 - y_{n-1}) = 1 + y$$

para algún $y \in \mathfrak{a}_n$; luego $(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) + \mathfrak{a}_n = A$, y tenemos:

$$(\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1})\mathfrak{a}_n = (\mathfrak{a}_1 \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n = (\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n.$$

(2). Tomamos $\mathfrak{a}_1$, $\mathfrak{a}_i$. Por hipótesis existe $x \in A$ tal que $f(x) = (1, 0, \ldots, 0)$, luego $x - 1 \in \mathfrak{a}_1$ y $x \in \mathfrak{a}_i$, y tenemos

$$1 = x - (x - 1) \in \mathfrak{a}_1 + \mathfrak{a}_i.$$

Recíprocamente, si $\mathfrak{a}_1 + \mathfrak{a}_i = A$, para $2 \leq i \leq n$, existen $x_i \in \mathfrak{a}_1$, $y_i \in \mathfrak{a}_i$ tales que $x_i + y_i = 1$. Definimos $x = y_2 \cdots y_n = (1 - x_2) \cdots (1 - x_n) = 1 + x'$ para algún $x' \in \mathfrak{a}_1$, luego $f(x) = (1, 0. \ldots, 0)$.
(3). Es evidente. □

4. Ideales primos e ideales maximales

Sea A un anillo, un elemento $a \in A$ se llama un **divisor de cero** si existe un elemento no nulo $b \in A$ tal que $ab = 0$. Los elementos de A que no son divisores de cero se llaman **elementos regulares**.

Cuando el elemento cero es el único divisor de cero de un anillo A, se dice que A es un **dominio de integridad**, ó simplemente un **dominio**.

Un elemento a de un anillo A se llama **nilpotente** si existe un entero positivo $n \in \mathbb{N}^{-1}$ tal que $a^n = 0$.

Ejercicio. 4.1.
Prueba que los elementos nilpotentes de un anillo forman un ideal.

Sea A un anillo, un ideal propio $\mathfrak{p}$ de A se llama un **ideal primo** si para cualesquiera $a, b \in A$ tales que $ab \in \mathfrak{p}$, se tiene $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$.

Ejemplo. 4.2.
En el caso del anillo $\mathbb{Z}$ de los números enteros los ideales primos son:

(I) el ideal cero y
(II) los ideales de la forma $p\mathbb{Z}$, siendo p un entero primo (positivo).

Lema. 4.3.
Sea A un anillo y $\mathfrak{p}$ un ideal propio, las siguientes condiciones son equivalentes:

(a) $\mathfrak{p}$ es un ideal primo;
(b) $A/\mathfrak{p}$ es un dominio de integridad.

DEMOSTRACIÓN. Supongamos que $\mathfrak{p}$ es un ideal primo, y sea $(a+\mathfrak{p})(b+\mathfrak{p}) = 0$, entonces $ab \in \mathfrak{p}$, y ya que $\mathfrak{p}$ es primo, tenemos $a \in \mathfrak{p}$ ó $b \in \mathfrak{p}$, entonces $a + \mathfrak{p} = 0$ ó $b + \mathfrak{p} = 0$. La otra implicación es similar. □

Estudiamos ahora cómo cambian los ideales primos en un cambio de anillo.

Lema. 4.4.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, se verifica:

(1) Si $\mathfrak{q}$ es un ideal primo de B, entonces $f^{-1}(\mathfrak{q})$ es un ideal primo A.
(2) Existe una correspondencia biyectiva entre los ideales de A que contienen a $\mathrm{Ker}(f)$ y los ideales de $\mathrm{Im}(f)$.
(3) En esta correspondencia la imagen y la preimagen de ideales primos son también ideales primos.

DEMOSTRACIÓN. (1). Sean $a, b \in A$ tales que $ab \in f^{-1}(\mathfrak{p})$, entonces se verifica $f(a)f(b) = f(ab) \in ff^{-1}(\mathfrak{p}) \subseteq \mathfrak{p}$, luego $f(a) \in \mathfrak{p}$ ó $f(b) \in \mathfrak{p}$, y tenemos $a \in f^{-1}(\mathfrak{p})$ ó $b \in f^{-1}(\mathfrak{p})$.
(2). Si $\mathfrak{b} \subseteq B$ es un ideal, entonces $f^{-1}(\mathfrak{b}) \supseteq \operatorname{Ker}(f)$ es un ideal. Por otro lado, si $\mathfrak{a} \supseteq \operatorname{Ker}(f)$ es un ideal, entonces $f(\mathfrak{a})$ es un ideal de $\operatorname{Im}(f)$. Sólo falta ver que estas aplicaciones son, una inversa de la otra.
(3). Es claro. □

Observa que la siguiente propiedad es en realidad una nueva caracterización de ideales primos.

Teorema. 4.5.
Sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales de A y $\mathfrak{p}$ un ideal primo de A, si $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n \subseteq \mathfrak{p}$, entonces existe un índice i tal que $\mathfrak{a}_i \subseteq \mathfrak{p}$.
Además si $\mathfrak{p} = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$, entonces $\mathfrak{a}_i = \mathfrak{p}$ para algún índice i.

DEMOSTRACIÓN. Si $\mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n \subseteq \mathfrak{p}$, y para cada índice i se verifica $\mathfrak{a}_i \nsubseteq \mathfrak{p}$, entonces existe $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$, y tenemos $x_1 \cdots x_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subseteq \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n \subseteq \mathfrak{p}$, y como $\mathfrak{p}$ es primo, existe un índice i tal que $x_i \in \mathfrak{p}$, lo que es una contradicción. □

Ver también Ejercicio (8.27.).

Ideales maximales

Sea A un anillo, un ideal propio $\mathfrak{m}$ de A se llama **maximal** si para cada ideal propio $\mathfrak{a}$ de A tal que $\mathfrak{m} \subseteq \mathfrak{a} \subsetneqq A$ se tiene $\mathfrak{m} = \mathfrak{a}$.

Lema. 4.6.
Sea A un anillo y $\mathfrak{m}$ un ideal propio, las siguientes condiciones son equivalentes:
(a) $\mathfrak{m}$ es un ideal maximal;
(b) $A/\mathfrak{m}$ es un cuerpo.

De la misma forma que en el caso de ideales primos, vamos a estudiar el comportamiento de los ideales maximales respecto a un homomorfismo de anillos.

Lema. 4.7.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces la correspondencia descrita en el Lema (4.4.) establece una correspondencia biyectiva entre los ideales maximales de A que contienen a $\operatorname{Ker}(f)$ y los ideales maximales $\operatorname{Im}(f)$.

Ejercicio. 4.8.
En general, dado un homomorfismo de anillos $f : A \longrightarrow B$*, si* $\mathfrak{m}$ *es un ideal maximal de* B*, no necesariamente* $f^{-1}(\mathfrak{m})$ *es un ideal maximal de* A*. Dar un ejemplo.*

Lema. 4.9. (Teorema de Krull.)
Sea A *un anillo, existe al menos un ideal maximal de* A*.*

DEMOSTRACIÓN. Se considera el conjunto $\Gamma = \{\mathfrak{a} \mid \mathfrak{a} \text{ es un ideal propio de } A\}$. El conjunto Γ es no vacío, ya que $0 \in \Gamma$, y está ordenado por la inclusión. Cada cadena en Γ tiene una cota superior en Γ, ya que la unión de una cadena de ideales propios es un ideal propio. Luego en Γ existen elementos maximales. Es claro que cada elemento maximal de Γ es un ideal maximal. □

Corolario. 4.10.
Sean A *un anillo y* $\mathfrak{a}$ *un ideal propio de* A*, entonces existe un ideal maximal* $\mathfrak{m}$ *de* A *tal que* $\mathfrak{a} \subseteq \mathfrak{m}$*.*

DEMOSTRACIÓN. [2] Basta considerar el anillo cociente $A/\mathfrak{a}$ y la correspondencia establecida en el Lema (4.4.). □

Corolario. 4.11.
Sea A *un anillo y* $x \in A$ *un elemento que no es invertible en* A*, existe un ideal maximal* $\mathfrak{m}$ *de* A *tal que* $x \in \mathfrak{m}$*.*

DEMOSTRACIÓN. Basta considerar el ideal (x), que es propio por no ser x invertible. □

[2] El teorema de Krull nos asegura la existencia de un ideal maximal $\mathfrak{m}$ que contiene a un ideal dado $\mathfrak{a}$. Sin embargo, no nos aporta nada al conocimiento de este ideal maximal. Por ejemplo, al considerar el anillo $A = \mathbb{Z}_2^{\mathbb{N}}$, tenemos que para cada $t \in \mathbb{N}$, el conjunto $\mathfrak{m}_t = \prod_{n\in\mathbb{N}} A_n$, siendo $A_n = \mathbb{Z}_2$ si $n \neq t$, y $A_t = 0$, es un ideal maximal, pues $A/\mathfrak{m}_t \cong \mathbb{Z}_2$. Por otro lado, el ideal $\mathfrak{b} = \mathbb{Z}_2^{(\mathbb{N})} \subseteq \mathbb{Z}_2^{\mathbb{N}}$ no está contenido en ningún ideal maximal $\mathfrak{m}_t$, pero está contenido en algún ideal maximal $\mathfrak{m}$. ¿Cómo describir uno de estos ideales maximales $\mathfrak{m}$?

Anillos locales

Un anillo A se llama **local** si tiene un único ideal maximal, o equivalentemente, si los elementos no invertibles forman un ideal. Si A es un anillo local con ideal maximal $\mathfrak{m}$, entonces el cuerpo $A/\mathfrak{m}$ se llama el **cuerpo residual** de A.

Lema. 4.12.
Sea A un anillo y $\mathfrak{m}$ un ideal propio de A, son equivalentes:
(a) cada elemento $x \in A \setminus \mathfrak{m}$ es invertible,
(b) A es un anillo local con ideal maximal $\mathfrak{m}$.

DEMOSTRACIÓN. Dado un ideal propio $\mathfrak{a}$ de A, los elementos de $\mathfrak{a}$ no son invertibles, luego $\mathfrak{a} \subseteq \mathfrak{m}$. □

Lema. 4.13.
Sea A un anillo y $\mathfrak{m}$ un ideal maximal de A tal que cada elemento $x \in 1+\mathfrak{m}$ es invertible, entonces A es un anillo local.

DEMOSTRACIÓN. Dado $x \in A \setminus \mathfrak{m}$, tenemos $\mathfrak{m}+Ax = A$, y existen $m \in \mathfrak{m}$, $a \in A$ tales que $m+ax = 1$, luego $ax = 1-m \in 1+\mathfrak{m}$. Entonces ax es invertible, y por tanto x también lo es. Aplicando el Lema (4.12.) tenemos el resultado. □

Un anillo A es un **anillo semilocal** si tiene un número finito de ideales maximales.
Dados dos anillos $A \subseteq B$, decimos que B **domina** a A si para cada ideal maximal $\mathfrak{m} \subseteq B$ se tiene que $\mathfrak{m} \cap A \subseteq A$ es un ideal maximal.

Teorema de elusión

Proposición. 4.14. (Teorema de elusión)
Sea A un anillo, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos de A y $\mathfrak{a}$ un ideal de A tal que $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$, entonces existe un índice i tal que $\mathfrak{a} \subseteq \mathfrak{p}_i$.

DEMOSTRACIÓN. Hacemos inducción sobre n. Para $n = 1$ el resultado es cierto. Supongamos que sea cierto para $n-1$ ($n \geq 2$), y sea $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ para cada índice i. Entonces

$$\mathfrak{a} \nsubseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_{i-1} \cup \mathfrak{p}_{i+1} \cup \ldots \cup \mathfrak{p}_n$$

y existe $x_i \in \mathfrak{a} \setminus \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_{i-1} \cup \mathfrak{p}_{i+1} \cup \ldots \cup \mathfrak{p}_n$. Si $x_i \notin \mathfrak{p}_i$, entonces $\mathfrak{a} \nsubseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$ y hemos terminado. Supongamos entonces que $x_i \in \mathfrak{p}_i$ para cada índice i. Definimos

$$y = \sum_{i=1}^{n} x_1 \cdots x_{i-1} x_{i+1} \cdots x_n;$$

tenemos $y \in \mathfrak{a}$ e $y \notin \mathfrak{p}_i$ para cada índice i, luego $\mathfrak{a} \nsubseteq \mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_n$. □

Un enunciado alternativo es:

Proposición. 4.15.
Sea $\mathfrak{a} \subseteq A$ un ideal y $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos tales que $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ para cada $i = 1, \ldots, n$, existe $a \in \mathfrak{a}$ tal que $a \notin \mathfrak{p}_i$ para cada i.

Extensiones del Teorema de elusión (*)

Los siguiente resultados son de aplicación en contextos más específicos; los incluimos aquí para ver posibles extensiones de la teoría.

Teorema. 4.16.
Sea A un anillo y $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales. Si se verifica una de las dos condiciones:
(1) a lo más dos de estos ideales no son primos, cuando $n > 2$, o
(2) A contiene un cuerpo infinito,

para cada ideal $\mathfrak{a}$ tal que $\mathfrak{a} \subseteq \cup_{i=1}^{n} \mathfrak{p}_i$ existe un índice i tal que $\mathfrak{a} \subseteq \mathfrak{p}_i$.

DEMOSTRACIÓN. (1). Hacemos inducción sobre n. Si $n = 1$, el resultado es cierto. Si $n = 2$, y $\mathfrak{a} \nsubseteq \mathfrak{p}_i$, $i = 1, 2$, existen $x_1 \in \mathfrak{a} \setminus \mathfrak{p}_2$, $x_2 \in \mathfrak{a} \setminus \mathfrak{p}_1$; observar que entonces $x_i \in \mathfrak{p}_i$, $i = 1, 2$. Entonces $y = x_1 + x_2 \notin \mathfrak{p}_1 \cup \mathfrak{p}_2$. Supongamos ahora que $n > 2$. Consideramos $\mathfrak{p}_1$ primo y si $\mathfrak{a} \nsubseteq \mathfrak{p}_i$, para cada índice i, existe $x_i \in \mathfrak{a} \setminus \mathfrak{p}_1 \cup \ldots \mathfrak{p}_{i-1} \cup \mathfrak{p}_{i+1} \cup \ldots \cup \mathfrak{p}_n$. Si $x_i \notin \mathfrak{p}_i$, entonces $\mathfrak{a} \nsubseteq \cup_{i=1}^{n} \mathfrak{p}_i$, lo que es una contradicción. Por tanto para cada índice i se tiene $x_i \in \mathfrak{p}_i$. En particular $x_2 \cdots x_n \in \mathfrak{p}_i$, $2 \leq i \leq n$, y definimos $y = x_1 + x_2 \cdots x_n \in \mathfrak{p}_i$, $2 \leq i \leq n$. Como $\mathfrak{p}_1$ es primo y resulta que $x_i \notin \mathfrak{p}_1$, $2 \leq i \leq n$, entonces $x_2 \cdots x_n \notin \mathfrak{p}_1$. Como $x_1 \in \mathfrak{p}_1$, resulta $y \notin \mathfrak{p}_1$. Entonces $y \notin \cup_{i=1}^{n} \mathfrak{p}_i$, lo que es una contradicción.
(2). Si $\mathfrak{a} \subseteq \cup_{i=1}^{n} \mathfrak{p}_i$, entonces $\mathfrak{a} = \cup_{i=1}^{n} (\mathfrak{a} \cap \mathfrak{p}_i)$ es un espacio vectorial propio que es una unión de espacios vectoriales; esto es una contradicción. □

Radicales

Sea A un anillo, llamamos **nilradical** de A al conjunto de todos los elementos nilpotentes de A, y lo representamos por $\operatorname{Nil}(A)$, y también por $\mathfrak{n}(A)$.

Lema. 4.17.
Sea A un anillo, entonces $\operatorname{Nil}(A)$ es un ideal y el anillo cociente $A/\operatorname{Nil}(A)$ no tiene ningún elemento nilpotente no nulo, esto es, $\operatorname{Nil}(A/\operatorname{Nil}(A)) = 0$.

DEMOSTRACIÓN. Sean $a, b \in \operatorname{Nil}(A)$, entonces existe $n \in \mathbb{N}$ tal que $a^n = 0 = b^n$; entonces se verifica: $(a+b)^{2n} = 0$, y $a+b \in \operatorname{Nil}(A)$. Si tenemos ahora $c \in A$, entonces $(ca)^n = 0$ y $ca \in \operatorname{Nil}(A)$. □

Un anillo A con $\operatorname{Nil}(A) = 0$ se llama un **anillo reducido**.

Teorema. 4.18.
Para cada anillo A se tiene que $\operatorname{Nil}(A)$ es la intersección de todos los ideales primos de A.

DEMOSTRACIÓN. Llamamos N a la intersección de todos los ideales primos del anillo A. Si $x \in \operatorname{Nil}(A)$, entonces existe $n \in \mathbb{N}$ tal que $x^n = 0$, luego para cada ideal primo $\mathfrak{p}$ se tiene $x \in \mathfrak{p}$, y como consecuencia $x \in N$. Sea ahora $x \in N \setminus \operatorname{Nil}(A)$, llamamos

$$\Gamma = \{\mathfrak{a} \subseteq A \mid \ \forall n \geq 1,\ x^n \notin \mathfrak{a}\}$$

Ya que $0 \in \Gamma$, se tiene que $\Gamma \neq \varnothing$. Es claro que Γ está ordenado por la inclusión y que es inductivo, por tanto tiene un elemento maximal. Sea $\mathfrak{p} \in \Gamma$ maximal, y sean $a, b \in A$ tales que $ab \in \mathfrak{p}$, si $a, b \notin \mathfrak{p}$, entonces $\mathfrak{p} + Aa, \mathfrak{p} + Ab \notin \Gamma$, por lo tanto existen $n, m \in \mathbb{N}$ tales que $x^n \in \mathfrak{p} + Aa$ y $x^m \in \mathfrak{p} + Ab$, y se tiene $x^{n+m} \in (\mathfrak{p} + Aa)(\mathfrak{p} + Ab) = \mathfrak{p} + Aab \subseteq \mathfrak{p}$, lo que es una contradicción. □

Utilizando el Teorema (4.18.) como modelo podemos definir un análogo al nilradical. El **radical de Jacobson** de un anillo A, que se define como la intersección de todos los ideales maximales de A, y que se representa por $\operatorname{Rad}(A)$ y también por $\mathfrak{j}(A)$.

$$\operatorname{Rad}(A) = \cap\{\mathfrak{m} \subseteq A \mid \ \mathfrak{m} \text{ es un ideal maximal de } A\}.$$

Vamos a buscar una descripción de los elementos de $\operatorname{Rad}(A)$.

Proposición. 4.19.
Sea A un anillo, entonces las siguientes condiciones son equivalentes:

(a) $x \in \operatorname{Rad}(A)$;
(b) Para todo $a \in A$ el elemento $1 - ax$ es invertible en A.

DEMOSTRACIÓN. Supongamos que $x \in \operatorname{Rad}(A)$ y sea $a \in A$ tal que $1-ax$ no es invertible en A. Existe un ideal maximal $\mathfrak{m}$ tal que $1-ax \in \mathfrak{m}$, por la hipótesis $x \in \mathfrak{m}$, luego $\mathfrak{m} = (1) = A$, lo que es una contradicción. Por otro lado, sea $x \notin \operatorname{Rad}(A)$, entonces existe un ideal maximal $\mathfrak{m}$ tal que $x \notin \mathfrak{m}$, como consecuencia tenemos $\mathfrak{m} + Ax = A$ y existe $m \in \mathfrak{m}$ tal que $m + ax = 1$ para algún $a \in A$, entonces $1 - ax = m \in \mathfrak{m}$ no sería invertible en A. □

Lema. 4.20.
Sea A un anillo, entonces las siguientes condiciones son equivalentes:

(a) A es un anillo local;
(b) $A \setminus \operatorname{Rad}(A)$ es el conjunto de los elementos invertible en A;
(c) Existe un ideal propio $\mathfrak{a}$ de A tal que $A \setminus \mathfrak{a}$ está contenido en el conjunto de los elementos invertibles.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si A es un anillo local, entonces $\operatorname{Rad}(A)$ es el único ideal maximal de A, luego $A \setminus \operatorname{Rad}(A)$ es el conjunto de los elementos invertibles de A.
(b) $\Rightarrow$ (c). Basta tomar $\mathfrak{a} = \operatorname{Rad}(A)$.
(c) $\Rightarrow$ (a). Supongamos que $\mathfrak{a}$ es un ideal propio de A con $A \setminus \mathfrak{a}$ contenido en el conjunto de los elementos invertibles, entonces $\mathfrak{a}$ es un ideal maximal y contiene a cualquier otro ideal propio de A, por tanto A es un anillo local con ideal maximal $\mathfrak{a}$. □

Ejemplo. 4.21.
En el caso del anillo $\mathbb{Z}$ de los números enteros el nilradical es cero, ya que 0 es un ideal primo, y el radical de Jacobson es cero, ya que la intersección de todos los ideales maximales (los de la forma $p\mathbb{Z}$, con p un entero primo positivo) es igual a 0.

Observación. 4.22.
Para cada anillo A tenemos:

(1) $A/\operatorname{Nil}(A)$ es un subanillo del anillo producto $\prod\{A/\mathfrak{p} \mid \mathfrak{p} \subseteq A \text{ es primo}\}$; cada factor del producto es un dominio de integridad.
(2) $A/\operatorname{Rad}(A)$ es un subanillo del anillo producto $\prod\{A/\mathfrak{m} \mid \mathfrak{m} \subseteq A \text{ es primo}\}$; cada factor del producto es un cuerpo. En particular si A es un anillo semilocal con ideales maximales $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, entonces $A/\operatorname{Rad}(A) = \prod_{i=1}^n A/\mathfrak{m}_i$.

5. Radical de un ideal

Sea $\mathfrak{a}$ un ideal de un anillo A, llamamos **radical** de $\mathfrak{a}$ al conjunto

$$\operatorname{rad}(\mathfrak{a}) = \{x \in A \mid \exists n \in \mathbb{N},\ x^n \in \mathfrak{a}\}.$$

Lema. 5.1.
Sean A un anillo y $\mathfrak{a}$ un ideal propio de A, se verifica la igualdad:

$$\operatorname{rad}(\mathfrak{a})/\mathfrak{a} = \operatorname{Nil}(A/\mathfrak{a}).$$

Corolario. 5.2.
En la situación anterior se verifica:

$$\operatorname{rad}(\mathfrak{a}) = \cap\{\mathfrak{p} \mid \mathfrak{p} \text{ es un ideal primo de } A \text{ y } \mathfrak{p} \supseteq \mathfrak{a}\}.$$

Proposición. 5.3.
Sean A un anillo, $\mathfrak{a}$ y $\mathfrak{b}$ ideales de A y $\mathfrak{p}$ un ideal primo de A, se verifica:

(1) $\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{a})$.
(2) Si $\mathfrak{a} \subseteq \mathfrak{b}$, *entonces* $\operatorname{rad}(\mathfrak{a}) \subseteq \operatorname{rad}(\mathfrak{b})$.
(3) $\operatorname{rad}(\mathfrak{a}) = \operatorname{rad}(\operatorname{rad}(\mathfrak{a}))$.
(4) $\operatorname{rad}(\mathfrak{ab}) = \operatorname{rad}(\mathfrak{a} \cap \mathfrak{b}) = \operatorname{rad}(\mathfrak{a}) \cap \operatorname{rad}(\mathfrak{b})$.
(5) $\operatorname{rad}(\mathfrak{a}) = A$ *si, y sólo si,* $\mathfrak{a} = A$.
(6) $\operatorname{rad}(\mathfrak{a}+\mathfrak{b}) = \operatorname{rad}(\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}))$.
(7) $\operatorname{rad}(\mathfrak{p}^n) = \mathfrak{p}$ *para cada* $n \in \mathbb{N}^*$.

DEMOSTRACIÓN. (4). Se tiene la inclusión $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}, \mathfrak{b}$, y por tanto se tiene $\operatorname{rad}(\mathfrak{ab}) \subseteq \operatorname{rad}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \operatorname{rad}(\mathfrak{a}) \cap \operatorname{rad}(\mathfrak{b})$. Por otro lado, si $x \in \operatorname{rad}(\mathfrak{a}) \cap \operatorname{rad}(\mathfrak{b})$, existe $n \in \mathbb{N}$ tal que $x^n \in \mathfrak{a} \cap \mathfrak{b}$, y se tiene que $x^{2n} \in \mathfrak{ab}$, luego $x \in \operatorname{rad}(\mathfrak{ab})$.

(6). Se tiene $\mathfrak{a}+\mathfrak{b} \subseteq \operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b})$, y por tanto $\operatorname{rad}(\mathfrak{a}+\mathfrak{b}) \subseteq \operatorname{rad}(\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}))$. Por otro lado, si $x \in \operatorname{rad}(\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}))$, existe $n \in \mathbb{N}$ tal que $x^n \in \operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b})$. Sea $x^n = a + b$, con $a \in \operatorname{rad}(\mathfrak{a})$ y $b \in \operatorname{rad}(\mathfrak{b})$. Existe $m \in \mathbb{N}$ tal que $a^m \in \mathfrak{a}$ y $b^m \in \mathfrak{b}$, entonces $(x^n)^{2m} = (a+b)^{2m} \in \mathfrak{a}+\mathfrak{b}$, luego $x^{2mn} \in \mathfrak{a}+\mathfrak{b}$ y se tiene $x \in \operatorname{rad}(\mathfrak{a}+\mathfrak{b})$. □

Corolario. 5.4.
Sean A un anillo, y $\mathfrak{a}, \mathfrak{b}$ ideales de A, son equivalentes:
(a) $\operatorname{rad}(\mathfrak{a})$ *y* $\operatorname{rad}(\mathfrak{b})$ *son comaximales.*
(b) $\mathfrak{a}$ *y* $\mathfrak{b}$ *son comaximales.*

DEMOSTRACIÓN. Tenemos las siguientes igualdades:

$$\operatorname{rad}(\mathfrak{a}+\mathfrak{b}) = \operatorname{rad}(\operatorname{rad}(\mathfrak{a})+\operatorname{rad}(\mathfrak{b})) = \operatorname{rad}(A) = A,$$

luego $\mathfrak{a}+\mathfrak{b} = A$. □

Ideales primos minimales

Sea $\mathfrak{a}$ un ideal de un anillo A, un ideal primo $\mathfrak{p}$ es un **ideal primo minimal sobre** $\mathfrak{a}$ si $\mathfrak{a} \subseteq \mathfrak{p}$ y para cualquier otro ideal primo $\mathfrak{q}$ tal que $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$ se tiene $\mathfrak{q} = \mathfrak{p}$. Los ideales primos minimales sobre 0 en A son los ideales **primos minimales** de A.

Proposición. 5.5.
Sea A un anillo y $\mathfrak{a}$ un ideal propio de A, entonces existen ideales primos minimales sobre $\mathfrak{a}$ y cada ideal primo que contiene a $\mathfrak{a}$ contiene un ideal primo minimal sobre $\mathfrak{a}$.

DEMOSTRACIÓN. Definimos $\Gamma = \{\mathfrak{p} \mid \ \mathfrak{p}$ es un ideal primo que contiene a $\mathfrak{a}\}$. Es claro que Γ es no vacío, pues cada ideal propio de A está contenido en un ideal maximal, y por tanto en un ideal primo. Sea $\{\mathfrak{p}_i\}_i$ una cadena de ideales en Γ, entonces $\cup_i\mathfrak{p}_i$ es un ideal que contiene a $\mathfrak{a}$; vamos a ver que es primo. En efecto, si $ab \in \cup_i\mathfrak{p}_i$, existe un índice i tal que $ab \in \mathfrak{p}_i$, y como $\mathfrak{p}_i$ es primo se tiene $a \in \mathfrak{p}$ o $b \in \mathfrak{p}_i$, luego $\cup_i\mathfrak{p}_i$ es un ideal primo.
Si $\mathfrak{q} \supseteq \mathfrak{a}$ es un ideal primo, consideramos la familia

$$\Gamma_{\mathfrak{q}} = \{\mathfrak{p} \mid \ \mathfrak{p} \subseteq \mathfrak{q} \text{ es un ideal primo que contiene a } \mathfrak{a}\}.$$

□

Ver Ejercicio (8.31.).
En consecuencia para cada ideal $\mathfrak{a}$ el radical de $\mathfrak{a}$ es la intersección de todos los ideales primos minimales sobre $\mathfrak{a}$.

$$\operatorname{rad}(\mathfrak{a}) = \cap\{\mathfrak{p} \mid \ \mathfrak{p} \text{ es un ideal primo minimal sobre } \mathfrak{a}\}.$$

Este resultado será de interés en el caso en que solamente haya un número finito de ideales primos minimales que contienen a $\mathfrak{a}$.

6. Extensión y contracción de ideales

Sea $f : A \longrightarrow B$ un homomorfismo de anillos. Dado un ideal $\mathfrak{a}$ de A, llamamos **extensión** de $\mathfrak{a}$ al ideal de B generado por $f(\mathfrak{a})$, y lo representamos por $\mathfrak{a}^e$. Esto es; $\mathfrak{a}^e = Bf(\mathfrak{a})$. De la misma forma, para cada ideal $\mathfrak{b}$ de B, llamamos **contracción** de $\mathfrak{b}$ a la imagen inversa de $\mathfrak{b}$ en A, y lo representamos por $\mathfrak{b}^c$.

Proposición. 6.1.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos, entonces existen dos aplicaciones:

$$\begin{array}{ll}(-)^e : \{\textit{ideales de } A\} \longrightarrow \{\textit{ideales de } B\}, & \mathfrak{a} \mapsto \mathfrak{a}^e \\ (-)^c : \{\textit{ideales de } B\} \longrightarrow \{\textit{ideales de } A\}, & \mathfrak{b} \mapsto \mathfrak{b}^c\end{array}$$

*que definen una **conexión de Galois**, esto es;*

(1) Si $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ son ideales de A, entonces $\mathfrak{a}_1^e \subseteq \mathfrak{a}_2^e$, y si $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ son ideales de B, entonces $\mathfrak{b}_1^c \subseteq \mathfrak{b}_2^c$.
(2) Si $\mathfrak{a}$ es un ideal de A, entonces $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ y si $\mathfrak{b}$ es un ideal de B, entonces $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$.
(3) Si $\mathfrak{a}$ es un ideal de A, entonces $\mathfrak{a}^e = \mathfrak{a}^{ece}$ y si $\mathfrak{b}$ es un ideal de B, entonces $\mathfrak{b}^c = \mathfrak{b}^{cec}$.
(4) Si $\mathcal{A}$ es el conjunto de los ideales contraídos en A y $\mathcal{B}$ es el conjunto de los ideales extendidos en B, entonces se tiene $\mathcal{A} = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $\mathcal{B} = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$ y existe una biyección de $\mathcal{A}$ a $\mathcal{B}$.

Proposición. 6.2.
Sean $f : A \longrightarrow B$ un homomorfismo de anillos, $\mathfrak{a}_1, \mathfrak{a}_2$ ideales de A y $\mathfrak{b}_1, \mathfrak{b}_2$ ideales de B, se verifica:

(1) $(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e$ *y* $(\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$.
(2) $(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e$ *y* $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$.
(3) $(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$ *y* $(\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$.
(4) $(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$ *y* $(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$.
(5) $\operatorname{rad}(\mathfrak{a}_1)^e \subseteq \operatorname{rad}(\mathfrak{a}_1^e)$ *y* $\operatorname{rad}(\mathfrak{b}_1)^c = \operatorname{rad}(\mathfrak{b}_1^c)$.

7. Álgebras

Sea A un anillo. Una A**–álgebra** es un anillo B junto con un homomorfismo de anillos $f : A \longrightarrow B$. Como consecuencia una A–álgebra es un anillo B que tiene estructura de A–módulo y que verifica la siguiente condición de compatibilidad:

$$a_1(ba_2) = (a_1b)a_2 \qquad \text{para todos } a_1, a_2 \in A \text{ y } b \in B.$$

Si B y C son A–álgebras, un **homomorfismo de** A**–álgebras** de B a C es un homomorfismo de anillos $f : B \longrightarrow C$ que es también homomorfismo de A–módulos.

El ejemplo más conocido de A-álgebra se tiene cuando $A = \mathbb{Z}$: *todo anillo es una* $\mathbb{Z}$*-álgebra*.

Como ya hemos visto, para cada anillo A existe un único homomorfismo de anillos $f : \mathbb{Z} \longrightarrow A$, el núcleo es de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{N}$. El número entero n se llama la **característica** de A. Observar que si $n \neq 0$, entonces n es el menor entero positivo n tal que $na = 0$ para cada $a \in A$.

Anillos de polinomios

Para cada anillo A existe una forma simple de construir una A–álgebra, y es considerar $A[X]$, el **anillo de polinomios** en la indeterminada X con coeficientes en A. Recordar que el anillo $A[X]$ se construye como el conjunto de todas las expresiones formales del tipo

$$a_0 + a_1X + \cdots + a_nX^n,$$

en donde $a_i \in A$. En $A[X]$ se definen dos operaciones que le dan estructura de anillo, y la aplicación $p : A \longrightarrow A[X]$, $p(a) = a$ es un homomorfismo de anillos.

El par $(p, A[X])$ verifica la siguiente propiedad universal:

Teorema. 7.1. (Propiedad universal del anillo de polinomios.)
Para cada anillo B, cada homomorfismo de anillos $f : A \to B$ y cada elemento $b \in B$, existe un único homomorfismo de anillos $f_b : A[X] \longrightarrow B$ tal que $f_b(X) = b$ y $f = f_b \circ p$.

$$\begin{array}{ccc} A & \xrightarrow{p} & A[X] \\ & {}_{f}\searrow \quad \swarrow_{\exists_1 f_b} & \\ & B & \end{array}$$

El homomorfismo f_b se llama el **homomorfismo de evaluación** en $X = b$.

Observar que el anillo de polinomios con coeficientes en A en las indeterminadas $X_1, \ldots, X_n$ se puede construir de forma recursiva como $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$. Por tanto los elementos de

$A[X_1,\ldots,X_n]$ admiten una expresión $\sum_i a_iX_n^i$, siendo $a_i \in A[X_1,\ldots,X_{n-1}]$ casi todos nulos. También podemos escribir los elementos de $A[X_1,\ldots,X_n]$ en la forma

$$\sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n},$$

con $a_{i_1,\ldots,i_n} \in A$ casi todos nulos.

El anillo de polinomios en varias indeterminadas tiene también una propiedad universal similar a la enunciada en el Teorema (7.1.).

Teorema. 7.2. (Propiedad universal del anillo de polinomios.)
Para cada anillo B, cada homomorfismo de anillos $f\colon A \to B$ y cada lista de n elementos $b_1,\ldots,b_n \in B$, existe un único homomorfismo de anillos $f_{b_1,\ldots,b_n}\colon A[X_1,\ldots,X_n] \longrightarrow B$ tal que $f_{b_1,\ldots,b_n}(X_i) = b_i$ para cada índice i y $f = f_{b_1,\ldots,b_n} \circ p$.

$$\begin{array}{ccc} A & \xrightarrow{\;p\;} & A[X_1,\ldots,X_n] \\ & {\scriptstyle f}\searrow & \swarrow {\scriptstyle \exists_1 f_{b_1,\ldots,b_n}} \\ & B & \end{array}$$

El homomorfismo $f_{b_1,\ldots,b_n}$ se llama el **homomorfismo de evaluación** en $X_1 = b_1,\ldots,X_n = b_n$.

Sobre la aritmética de los anillos de polinomios ver los Ejercicios (8.62.) y (8.63.).

Dado un anillo A y un conjunto Λ, si consideramos un conjunto de indeterminadas indizado en Λ, $\{X_\alpha \mid \alpha \in \Lambda\}$, el anillo de polinomios con coeficientes en A en las indeterminadas $\{X_\alpha \mid \alpha \in \Lambda\}$ se define como la unión de los anillos $B = \cup\{A[X_\alpha \mid \alpha \in F \subseteq \Lambda] \mid F \text{ finito}, F \subseteq \Lambda\}$. Si se definen en B la suma y el producto en la forma obvia, cada inclusión $A[X_\alpha \mid \alpha \in F \subseteq \Lambda] \subseteq B$ es un homomorfismo de anillos. El anillo B se representa por $A[\{X_\alpha \mid \alpha \in \Lambda\}]$, y se llama el **anillo de polinomios** en las indeterminadas $\{X_\alpha \mid \alpha \in \Lambda\}$.

Si A es un anillo, una A–álgebra B se llama **finitamente generada** si existe un homomorfismo sobreyectivo de un anillo de polinomios, con coeficientes en A en un número finito de indeterminadas, a B. O equivalentemente, si existen elementos $b_1,\ldots,b_t \in B$, tales que cualquier elemento $b \in B$ se escribe como una suma finita en la forma $b = \sum_{\alpha\in\mathbb{N}^t} c_\alpha b_1^{\alpha_1}\cdots b_t^{\alpha_t}$, siendo $\alpha = (\alpha_1,\ldots,\alpha_t) \in \mathbb{N}^t$, y $c_\alpha \in A$, casi todos nulos.

Sea K un cuerpo y B una K–álgebra. Un conjunto de n elementos $b_1,\ldots,b_n \in B$ se dice que es **algebraicamente independiente** sobre K si para cada polinomio $F \in K[X_1,\ldots,X_n]$ tal que $F(b_1,\ldots,b_n) = 0$ se tiene que $F = 0$. Vamos a caracterizar las listas de elementos algebraicamente independientes como aquellas que generan subanillos que son isomorfos a anillos de polinomios. Tenemos la siguiente proposición:

Proposición. 7.3.
Sea K un cuerpo y B una K–álgebra. Para una lista $b_1,\ldots,b_n$ de elementos de B son equivalentes los siguientes enunciados:

(a) $b_1,\ldots,b_n$ es algebraicamente independiente;
(b) El homomorfismo $f_{b_1,\ldots,b_n}: K[X_1,\ldots,X_n] \longrightarrow B$, definido por la propiedad universal, es inyectivo.

DEMOSTRACIÓN. $(a) \Rightarrow (b)$. Siguiendo con la notación de la propiedad universal del anillo de polinomios el homomorfismo de evaluación para $X_1 = b_1,\ldots,X_n = b_n$ es inyectivo, pues si $F \in \operatorname{Ker}(f_{b_1,\ldots,b_n})$, entonces $F(b_1,\ldots,b_n) = 0$ y al ser los $b_1,\ldots,b_n$ algebraicamente independientes se tiene $F = 0$.
$(b) \Rightarrow (a)$. Es inmediato. □

Anillos de series formales de potencias (*)

Sea A un anillo y X una indeterminada. Una **serie formal de potencias** en X con coeficientes en A es una expresión formal $\sum_{i=0}^{\infty} a_iX^i$. Llamamos $A[[X]]$ al conjunto de las series formales de potencias en X con coeficientes en A.
En el conjunto $A[[X]]$ de las series formales de potencias se definen dos operaciones:

$$(\sum_{i=0}^{\infty} a_iX^i) + (\sum_{i=0}^{\infty} b_iX^i) = \sum_{i=0}^{\infty}(a_i + b_i)X^i;$$

$$(\sum_{i=0}^{\infty} a_iX^i)(\sum_{i=0}^{\infty} b_iX^i) = \sum_{i=0}^{\infty} c_iX^i, \text{ con } c_i = \sum_{j+k=i} a_jb_k.$$

Si para cada elemento $a \in A$ consideramos la serie formal $a + 0X + 0X^2 + \cdots$, podemos definir un homomorfismo de anillos $A \to A[[X]]$, e identificar A con su imagen en $A[[X]]$.

Teorema. 7.4.
Para cada anillo A y cada indeterminada X el conjunto $A[[X]]$ con las operaciones anteriores y elemento uno igual a 1 es un anillo.

El anillo $A[[X]]$ se llama el **anillo de las series formales de potencias** en X con coeficientes en A.
Cada polinomio $F \in A[x]$ puede ser considerado una serie formal de potencias, por lo tanto podemos suponer que $F \in A[[X]]$. Se tiene entonces:

Proposición. 7.5.
Para cada anillo A y cada indeterminada X el anillo de polinomios $A[X]$ es un subanillo del anillo de series formales de potencias $A[[X]]$.

Podemos extender la construcción del anillo de series formales potencias a un número finito de indeterminadas, $X_1, \ldots, X_t$, para ello definimos $A[[X_1, \ldots, X_t]] = A[[X_1, \ldots, X_{t-1}]][[X_t]]$.
Observa que los anillos de series formales de potencias, tanto $A[[X]]$ como $A[[X_1, \ldots, X_t]]$, se pueden también definir a partir de los anillos de polinomios $A[X]$ ó $A[X_1, \ldots, X_t]$ en la siguiente forma:

$$A[[X_1, \ldots, X_t]] = \{\sum_{i=0}^{\infty} F_i \mid F_i \in A[X_1, \ldots, X_t]\}.$$

Sobre la aritmética de los anillos de series de potencias ver el Ejercicio (8.69.).

Mientras el Teorema de McCoy, ver Ejercicio (8.57.), caracteriza los divisores del cero de un anillo de polinomios, no existe un teorema similar en el caso de anillos de series formales de potencias. Veamos un ejemplo de un divisor de cero.

Ejemplo. 7.6.
Se considera un cuerpo K, el anillo de polinomios $K[Y, Z_0, Z_1, Z_2, \ldots]$ y el ideal $\mathfrak{a} = (YZ_0) + (Z_n + YZ_{n+1} \mid n \in \mathbb{N})$. Llamamos $A = K[Y, Z_0, Z_1, Z_2, \ldots]/\mathfrak{a} = K[y, z_0, z_1, z_2, \ldots]$ y consideramos $F = y + X \in A[[X]]$. Vamos a ver que F es un divisor de cero; para ello basta ver que

$$(y + X)(z_0 + z_1 X + \cdots + z_n X^n + \cdots) = 0.$$

Sin embargo, para un tipo especial de anillos se tiene un resultado similar el Teorema de McCoy.

Teorema. 7.7.
Sea A un anillo reducido, esto es, $\mathrm{Nil}(A) = 0$. *Sean* $F = \sum_{i=0}^{\infty} a_i X^i, G = \sum_{i=0}^{\infty} b_i X^i \in A[[X]]$. *Son equivalentes:*

(a) $FG = 0$,
(b) $a_i b_j = 0$ *para todos* i, j.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $FG = 0$, vamos a probar que $a_0 b_j = 0$ para todo j. Hacemos la demostración por inducción sobre j. Para $j = 0$ el resultado es cierto. Supongamos que sea cierto para $j = 0, 1, \ldots, t-1$. El coeficiente de X^t en FG es:

$$0 = a_0 b_t + a_1 b_{t-1} + \cdots + a_{t-1} b_1 + a_t b_0.$$

Multiplicando por a_0 se tiene:

$$0 = a_0(a_0 b_t + a_1 b_{t-1} + \cdots + a_{t-1} b_1 + a_t b_0) = a_0^2 b_t,$$

y de aquí $0 = (a_0 b_t)^2$. Como A es un anillo reducido, se tiene $a_0 b_t = 0$. Llamamos F' a la serie formal de potencias tal que $XF' = F - a_0$, Se verifica $F'G = 0$, y por tanto $a_1 b_j = 0$ para cada j. Repitiendo el proceso se tiene $a_i b_j = 0$ para cada i y cada j. □

Problema. 7.8.
Calcular $\operatorname{Nil}(A[[X]])$.

Vamos a calcular ahora los ideales maximales de $A[[X]]$. Se tiene:

Teorema. 7.9.
Los ideales maximales de $A[[X]]$ *son de la forma* $\mathfrak{m} + (X)$, *siendo* $\mathfrak{m}$ *un ideal maximal de* A.
En consecuencia, si A *es un cuerpo o un anillo local, entonces* $A[[X]]$ *es un anillo local.*

DEMOSTRACIÓN. (1). Para cada ideal maximal $\mathfrak{m} \subseteq A$ se tiene que $\mathfrak{m} + (X)$ es un ideal maximal. Basta considerar el homomorfismo $\varepsilon : A[[X]] \longrightarrow A$ definido $\varepsilon(\sum_{i=0}^{\infty} a_i X^i) = a_0$ y la biyección entre los ideales de A y los ideales de $A[[X]]$ que contiene a $\operatorname{Ker}(\varepsilon) = (X)$.
(2). Para cada ideal maximal $\mathfrak{n} \subseteq A[[X]]$ definimos $\mathfrak{m} = \varepsilon(\mathfrak{n})$. Es claro que $\mathfrak{m}$ es un ideal de A ya que ε es sobreyectiva, y es un ideal maximal, ya que si $a \in A \setminus \mathfrak{m}$, entonces $a \notin \mathfrak{n}$, y se tiene $\mathfrak{n} + aA[[X]] = A[[X]]$, luego existen $F = \sum_{i=0}^{\infty} a_i X^i \in \mathfrak{n}$ y $G = \sum_{i=0}^{\infty} b_i X^i \in A[[X]]$ tales que $F + aG = 1$, en particular $a_0 + ab_0 = 1$ y por tanto $\mathfrak{m} + aA = A$.
(3). Es claro que $\mathfrak{m} + (X) \subseteq \mathfrak{n}$, y como $\mathfrak{m} + (X)$ es maximal, se tiene la igualdad. □

En general si A es un domino de factorización única, el anillo de polinomios $A[X]$ es un dominio de factorización única. Esta propiedad no es cierta para anillos de series formales de potencias; este resultado fue dado por P. Samuel en 1961. Sin embargo con algunas restricciones el resultado es cierto.

Teorema. 7.10.
Si D *es un dominio de ideales principales, el anillo de series de potencias formales* $D[[X]]$ *es un dominio de factorización única.*

La demostración se basa en dos lemas debidos a I. Kaplansky. El primero es el Corolario (28.13.), y el segundo es:

Lema. 7.11. (Kaplansky.)
Sea D *un dominio de integridad. Son equivalentes:*

(a) D *es un dominio de factorización única.*
(b) Cada ideal primo no nulo de D *contiene un elemento primo.*

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Es claro.
(b) $\Rightarrow$ (a). Vamos a ver que cada elemento no nulo y no invertible es un producto de elementos primos, y por el Lema (**??**) será un DFU. Llamamos C al conjunto

$$C = \{x \in D \mid \; x \text{ es no nulo, no invertible y es un producto de elementos primos}\}.$$

Dado $d \notin C$ no nulo y no invertible, procedemos como sigue:
(1). Probamos que $(d) \cap C = \varnothing$. Si $ad \in C$, se puede escribir $ad = p_1 \cdots p_t$, como producto de elementos primos. Se tiene $p_1 \mid a$ ó $p_1 \mid d$; podemos escribir entonces $a = p_1 a_1$ ó $d = p_1 d_1$. Tenemos entonces:

$$a_1 d = p_2 \cdots p_t \quad \text{ó} \quad ad_1 = p_2 \cdots p_t.$$

Ahora eliminamos p_2 de la misma forma. Tras t pasos obtenemos una expresión $a_i d_j = 1$, por lo tanto $d \in C$, lo que es una contradicción.
(2). Tomamos $\Gamma = \{\mathfrak{a} \subseteq D \mid \; d \in \mathfrak{a}, \; \mathfrak{a} \cap C = \varnothing\}$. Este conjunto es inductivo, luego por el Lema de Zorn tiene elementos maximales. Si $\mathfrak{a} \in \Gamma$ es maximal vamos a probar que es un ideal primo. Sean $a, b \in D$ tales que $ab \in \mathfrak{a}$; si $a, b \notin \mathfrak{a}$ existen $x \in (\mathfrak{a} + (a)) \cap C$ e $y \in (\mathfrak{a} + (b)) \cap C$, por tanto $xy \in (\mathfrak{a} + (a))(\mathfrak{a} + (b)) \subseteq \mathfrak{a}$ y $xy \in C$, lo que es una contradicción.
(3). Por la hipótesis $\mathfrak{a}$ contiene un elemento primo, luego $\mathfrak{a} \cap C \neq \varnothing$, lo que es una contradicción.
En consecuencia todo elemento no nulo y no invertible pertenece a C, y tenemos el resultado. □

DEMOSTRACIÓN. [del Teorema] Dado un ideal primo no nulo $\mathfrak{p} \subseteq D[[X]]$, si $X \in \mathfrak{p}$, entonces $\mathfrak{p}$ contiene un elemento primo. Si $X \notin \mathfrak{p}$, el ideal $\varepsilon(\mathfrak{p})$ es no nulo y está generado por un elemento, sea $\varepsilon(\mathfrak{p}) = (d)$. Podemos probar que $\mathfrak{p}$ está generado por un elemento. Sea $F \in \mathfrak{p}$ tal que $\varepsilon(F) = d$, si $G \in \mathfrak{p}$ se tiene $\varepsilon(G) = da_0$, luego $G - Fa_0 \in \operatorname{Ker}(\varepsilon)$, y existe $H \in D[[X]]$ tal que $XH = G - Fa_0 \in \mathfrak{p}$, luego $H \in \mathfrak{p}$. Aplicando el mismo argumento a H, existe a_1 tal que $H - Fa_1 \in \operatorname{Ker}(\varepsilon)$, y tenemos $G = Fa_0 + Fa_1 X + X^2 H'$ para algún $H' \in \mathfrak{p}$. Podemos deducir que $G \in (F)$ y se tiene $\mathfrak{p} = (F)$. Como $\mathfrak{p} = (F)$ es un ideal primo, F es un elemento primo. De esta forma cada ideal primo no nulo contiene un elemento primo, y el resultado se sigue aplicando el Lema (7.11.). □

Serie formal de potencias de Laurent

El anillo de series formales de potencias $A[[X]]$ se puede extender a un anillo más general, el anillo $A[[X^{-1}, X]]$ de las **series formales de potencias de Laurent**. Los elementos de este anillo son expresiones del tipo

$$\sum_{i=-t}^{\infty} a_i X^i,$$

donde $t \in \mathbb{N}$, $a_i \in A$. Las operaciones con estas series formales son análogas a las ya introducidas; de forma que $A[[X^{-1}, X]]$ es un anillo, y se tienen inclusiones $A[X] \subseteq A[[X]] \subseteq A[[X^{-1}, X]]$.
De forma análoga podemos definir el anillo de **series formales de potencias (descendentes) de Laurent** como el anillo $A[[X, X^{-1}]]$, cuyos elementos son expresiones formales del tipo

$$\sum_{i=t}^{-\infty} a_i X^i,$$

donde la suma es descendente para los índices.

Observa la diferencia en la notación de los dos anillos que acabamos de introducir.

Existe un nuevo anillo $A[X,X^{-1}]$, que se puede definir como $A[[X^{-1},X]] \cap A[[X,X^{-1}]]$; sus elementos son expresiones formales del tipo

$$\sum_{i=t}^{s} A_i X^i,$$

para enteros $t \leq s$, y $a_i \in A$, y se llaman **polinomios de Laurent** en X con coeficientes en A.

8. Ejercicios

Definición de anillo

Ejercicio. 8.1.
Sea X un conjunto, en $\mathcal{P}(X)$ se consideran las operaciones:

$$\begin{array}{l} A+B=(A\cup B)\setminus(A\cap B) \text{ y} \\ A\times B=A\cap B, \qquad\qquad . \end{array}$$

para cualesquiera $A,B\in\mathcal{P}(X)$.

(1) Prueba que $\mathcal{P}(X)$, con las operaciones anteriores y elemento uno igual a X, es un anillo conmutativo. ¿Cuál es el elemento cero?
(2) Observa que en este anillo se tiene $A^2=A$ para cada $A\in\mathcal{P}(X)$, y que por tanto se tiene $2A=0$.
*(3) Un anillo en el que para cada elemento a se tiene $a^2=a$ se llama un **anillo de Boole**.*

Ver Ejercicio (8.33.). *SOLUCIÓN*

Ejercicio. 8.2.
Dado un anillo $(A,+,\times,1)$, definir sobre A dos operaciones $\oplus$ y $\otimes$ de forma que $(A,\oplus,\otimes,0)$ sea un anillo con el elemento 1 como cero. Determina las propiedades que verifica este nuevo anillo.

SOLUCIÓN

Ejercicio. 8.3.
Se consideran $F_1,F_2,G\in K[X_1,\dots,X_n]$.

(1) Prueba que $((F_i):G)$ es un ideal principal. Determina un generador.
(2) Como $((F_i):G)\subseteq((F_1)+(F_2)):G$, entonces $((F_1):G)+((F_2):G)\subseteq((F_1)+(F_2)):G$. Estudia si es siempre cierta la igualdad.

SOLUCIÓN

Homomorfismos de anillos

Ejercicio. 8.4.
¿Se deduce la condición $f(1)=1$, en la definición de homomorfismo de anillos, de las dos condiciones $f(a+b)=f(a)+f(b)$ y $f(ab)=f(a)f(b)$ para todos $a,b\in A$?

En caso afirmativo da una demostración de este hecho, y en caso negativo da un ejemplo en el que no se verifique esta condición.

SOLUCIÓN

Ejercicio. 8.5.
Estudia los siguientes enunciados:

(1) *Si* $\mathbb{Z}[\sqrt{2}]$ *es el subanillo generado por* $\sqrt{2}$ *en* $\mathbb{C}$*, demuestra que* $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$.

(2) *Igual para* $\sqrt{3}$ *en vez de* $\sqrt{2}$.

(3) *Demuestra que no existe ningún homomorfismo de anillos de* $\mathbb{Z}[\sqrt{2}]$ *a* $\mathbb{Z}[\sqrt{3}]$.

SOLUCIÓN

Ejercicio. 8.6.
Sean $N \subseteq M$ *un submódulo de un* A*–módulo* M*, y* $a \in A$*,* $m \in M$*. Prueba que se verifica:*
(1) *Existe un isomorfismo* $\frac{N+Am}{N} \cong \frac{A}{(N:m)}$.
(2) *Existe un isomorfismo* $\frac{N+aM}{N} \cong \frac{M}{(N:a)}$.

Observa que hemos utilizado la siguiente notación: $(N : m) = \{a \in a \mid am \in N\}$ *es un ideal de* A*;* $(N : a) = \{m \in M \mid am \in N\}$ *es un submódulo de* M.

SOLUCIÓN

Ideales

Ejercicio. 8.7.
Dados ideales $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$*, prueba los siguientes resultados para los ideales residuales:*
(1) *Demuestra que* $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$ *es un ideal de* A *que contiene a* $\mathfrak{a}$.
(2) *Si* $\mathfrak{b} \subseteq \mathfrak{c}$*, entonces* $(\mathfrak{a} : \mathfrak{b}) \supseteq (\mathfrak{a} : \mathfrak{c})$.
(3) *Si* $\mathfrak{b} \subseteq \mathfrak{c}$*, entonces* $(\mathfrak{b} : \mathfrak{a}) \subseteq (\mathfrak{c} : \mathfrak{a})$.
(4) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$.
(5) $((\mathfrak{a} \cap \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{c}) \cap (\mathfrak{b} : \mathfrak{c})$.
(6) $(\mathfrak{a} : (\mathfrak{b} + \mathfrak{c})) = (\mathfrak{a} : \mathfrak{b}) \cap (\mathfrak{a} : \mathfrak{c})$.

Los resultados (4) y (5) son también válidos para intersecciones y sumas de conjuntos infinitos de ideales.

SOLUCIÓN

Ejercicio. 8.8.
En $\mathbb{Z}[X]$, para cada entero positivo k podemos encontrar ideales $\mathfrak{a}_k$ generados por k elementos y no por menos.

SOLUCIÓN

Ejercicio. 8.9.
Sean $m,n \in \mathbb{Z}$ enteros positivos.

(1) ¿Cuándo es cierto que $((m):(n)) = (m/n)$?
(2) ¿Cuándo es cierto que $((m):(n)) = (m)$?
(3) ¿Qué otros casos pueden ocurrir?

SOLUCIÓN

Ejercicio. 8.10.
Estudia los siguientes enunciados:

(1) Calcula $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_{30}, \mathbb{Z}_{21})$.
(2) Demuestra que $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_d$ donde $d = \mathrm{m.c.d.}\{n,m\}$.

SOLUCIÓN

Producto de anillos

Ejercicio. 8.11.
Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un anillo A.

*(1) Demuestra que $\mathfrak{a}+\mathfrak{b} = A$, si, y solo si, $\mathfrak{a}^n + \mathfrak{b}^n = A$ para cada entero positivo n. (Se dice que $\mathfrak{a}$ y $\mathfrak{b}$ son **ideales comaximales**.)*
(2) Demuestra que si $\mathfrak{a}+\mathfrak{b} = A$, entonces $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\cap\mathfrak{b}$.
(3) En este caso se tiene un isomorfismo de anillos $A/(\mathfrak{a}\cap\mathfrak{b}) \cong \frac{A}{\mathfrak{a}} \times \frac{A}{\mathfrak{b}}$.
(4) Demuestra que si $\mathfrak{a}, \mathfrak{b}$ son ideales propios comaximales, entonces $\mathfrak{a}, \mathfrak{b} \nsubseteq J(A)$.
(5) Demuestra que si $\mathfrak{a}_1, \ldots, \mathfrak{a}_t$ son ideales comaximales, entonces $\mathfrak{a}_1 + (\mathfrak{a}_2 \cdots \mathfrak{a}_t)^n = A$ para cada $t \in \mathbb{N}$.

SOLUCIÓN

Ejercicio. 8.12.
Sea $\{f_i : A_i \to B_i \mid i \in I\}$ *una familia de homomorfismos de anillos, entonces existe un único homomorfismo de anillos* $\prod_i f_i : \prod_i A_i \to \prod_i B_i$ *tal que* $f_j \circ \beta_{A_j} = \beta_{B_j} \circ (\prod_i f_i)$.

$$\begin{array}{ccc} \prod_i A_i & \xrightarrow{\prod_i f_i} & \prod_i B_i \\ \downarrow{\scriptstyle \beta_{A_j}} & & \downarrow{\scriptstyle \beta_{B_j}} \\ A_j & \xrightarrow{f_j} & B_j \end{array}$$

SOLUCIÓN

Ejercicio. 8.13.
Sea A *un anillo y* $\{\mathfrak{a}_i \mid i \in I\}$ *un conjunto independiente de ideales no nulos. Prueba que* I *es un conjunto finito.*

SOLUCIÓN

Ejercicio. 8.14.
Sea $A = \prod\{A_n \mid n \in \mathbb{N}\}$, *siendo* $A_n = \mathbb{Z}_2$ *para cada índice* n. *Se define* $\mathfrak{b}_t = \prod\{A_n \mid n \in \mathbb{N}\}$, *siendo* $A_n = \mathbb{Z}_2$ *si* $t = n$ *y* $A_n = 0$ *si* $t \neq n$.

(1) Prueba que $\{\mathfrak{b}_n \mid n \in \mathbb{N}\}$ *es una familia independiente de ideales de* A.
(2) Prueba que $\sum_{n\in\mathbb{N}} \mathfrak{b}_n \neq A$.
(3) Prueba que A *es un anillo descomponible.*

SOLUCIÓN

Ejercicio. 8.15.
Dado un con junto X *con operaciones suma y producto de forma que* $(X, +, \times)$ *verifica los axiomas de anillo, salvo, posiblemente, la existencia de uno, en* $X \times \mathbb{Z}$ *se definen las operaciones*

$$\begin{aligned} (x_1, n_1) + (x_2, n_2) &= (x_1 + x_2, n_1 + n_2), \\ (x_1, n_1) \times (x_2, n_2) &= (x_1x_2 + n_1x_2 + n_2x_1, n_1n_2). \end{aligned}$$

(1) Prueba que $(X \times \mathbb{Z}, +, \times, (0, 1))$ *es un anillo.*

(2) *Si identificamos* X *con* $\{(x,0) \in X\times\mathbb{Z} \mid x \in X\}$, *prueba que* $X \subseteq X\times\mathbb{Z}$ *es un ideal y que* $X\times\mathbb{Z}/X \cong \mathbb{Z}$. *Llamamos a* $X\times\mathbb{Z}$ *la* **extensión de Dorroh** *de* $\mathbb{Z}$.

(3) ***Propiedad universal de la extensión de Dorroh.*** *Prueba que para cualquier homomorfismo, para la suma y el producto,* $f : X \to B$ *a un anillo* B, *existe un único homomorfismo de anillos* $f' : X\times\mathbb{Z} \to B$ *tal que* $f'_{|X} = f$.

$$\begin{array}{ccc} X & \longrightarrow & X\times\mathbb{Z} \\ & \searrow^{f} & \downarrow \exists_1 f' \\ & & B \end{array}$$

SOLUCIÓN

Ejercicio. 8.16.
Sea A *un anillo, demuestra que* $A \cong B\times C$ *si y solo si existe un* **elemento idempotente** e, *esto es,* $e^2 = e$, *tal que* $B = eA$ *y* $C = (1-e)A$.

SOLUCIÓN

Ejercicio. 8.17.
Sea $A = \prod_{i=1}^{n} A_i$ *un producto de anillos.*

(1) *Demuestra que cada ideal de* A *es de la forma* $\prod_{i=1}^{n} \mathfrak{a}_i$, *donde cada* $\mathfrak{a}_i$ *es un ideal de* A_i, $i = 1,\dots,n$.
(2) *¿Cuáles son los ideales primos y los ideales maximales de* A?
(3) *Si los* A_i *son todos cuerpos demuestra que* A *tiene sólo un número finito deideales.*

SOLUCIÓN

Ejercicio. 8.18.
Se considera el anillo cociente $A = [X,Y]/(XY)$.

(1) *Prueba que cada elemento de* A *tiene un único representante de la forma* $k + F_1(X)X + F_2(Y)Y$, *siendo* $k \in K$, $F_1(X) \in K[X]$ *y* $F_2(Y) \in K[Y]$.
(2) *Describe la multiplicación de* A *en términos de los representantes antes mencionados.*
(3) *Determina los ideales maximales de* A.

SOLUCIÓN

Ejercicio. 8.19.
Dados dos anillos A y B, para el anillo producto $A \times B$ se tiene la siguiente situación:

$$A \underset{q_A}{\overset{j_A}{\rightleftarrows}} A \times B \underset{q_B}{\overset{j_B}{\leftrightarrows}} B$$

(1) Prueba que existen aplicaciones (homomorfismos de grupos abelianos) $j_A : A \longrightarrow A \times B$, definido $j_A(a) = (a, 0)$ para cada $a \in A$ y $j_B : B \longrightarrow A \times B$ definido $j_B(b) = (0, b)$ para cada $b \in B$.
(2) Prueba que existen homomorfismos de anillos $q_A : A \times B \longrightarrow A$, definido $q_A(a, b) = a$ para cada $(a, b) \in A \times B$ y $q_B : A \times B \longrightarrow B$, definido $q_B(a, b) = b$ para cada $(a, b) \in A \times B$.
(3) Prueba que para cada anillo X y cada par de homomorfismos de anillos $f_A : X \longrightarrow A$, $f_A : X \longrightarrow B$ existe un único homomorfismo de anillos $f : X \longrightarrow A \times B$ tal que $f_A = q_A \circ f$ y $f_B = q_B \circ f$.

$$\begin{array}{ccccc} & & X & & \\ & \swarrow^{f_A} & \downarrow{\exists_1 f} & {}^{f_B}\searrow & \\ A & \xleftarrow[q_A]{} & A \times B & \xrightarrow[q_B]{} & B \end{array}$$

Esto es, el par $(A \times B, \{q_A, q_B\})$ es un producto de los anillos A y B.
(4) Prueba que los elementos $e_A = (1, 0)$, $e_B = (0, 1) \in A \times B$ son idempotentes y verifican $e_A + e_B = (1, 1)$, y que de esto se deduce que $e_1e_2 = 0$.
(5) Dado un anillo C y dos elementos idempotentes $e_1, e_2 \in C$ tales que $e_1 + e_2 = 1$ definimos $C_1 = e_1C$ y $C_2 = e_2C$. Prueba que C_1 y C_2 son anillos (no subanillos de C) y que existe un isomorfismo $C \cong C_1 \times C_2$.
(6) Prueba que existe una biyección *entre pares (e_1, e_2) de elementos idempotentes de un anillo C verificando $e_1 + e_2 = 1$ y descomposiciones $C_1 \times C_2$ de C.*

SOLUCIÓN

Ejercicio. 8.20.
Se considera el anillo $A = K[X, Y]/(XY)$.
(1) Se considera la aplicación $f_X : K[X] \longrightarrow A$ definida por $f_X(X) = X + (XY)$. ¿Es f_X un homomorfismo de anillos? Estudia el caso de $f_Y : K[Y] \longrightarrow A$. ¿Puede identificarse $K[X]$ con un subanillo de A?
(2) Se considera la aplicación $g_X : A \longrightarrow K[X]$ definida por $g_X(k + F_1(X)X + F_2(Y)Y + (XY)) = k + F_1(X)X$. ¿Es g_X un homomorfismo de anillos? Estudia el caso de g_Y. Estudia su núcleo.
(3) ¿Existe algún homomorfismo de anillos α que hace conmutar el siguiente diagrama?

$$\begin{array}{ccccc} K[X] & \xleftarrow{g_X} & A & \xrightarrow{g_Y} & K[Y] \\ \downarrow{id} & & \downarrow{\alpha} & & \downarrow{id} \\ K[X] & \xleftarrow[q_{K[X]}]{} & K[X] \times K[Y] & \xrightarrow[q_{K[Y]}]{} & K[Y] \end{array}$$

En caso afirmativo, ¿cómo está definido α? Determina su imagen y su núcleo.

(4) *Observa que tenemos el siguiente cuadrado conmutativo de homomorfismos de anillos:*

$$\begin{array}{ccc} A & \xrightarrow{g_X} & K[X] \\ {\scriptstyle g_Y}\downarrow & & \downarrow{\scriptstyle eval_0} \\ K[Y] & \xrightarrow[eval_0]{} & K \end{array}$$

El anillo A y los homomorfismos g_X, g_Y verifican la siguiente propiedad universal: Para cada anillo B y cada par de homomorfismos $h_X : B \longrightarrow K[X]$ y $h_Y : B \longrightarrow K[Y]$ tales que $eval_0 \circ h_X = eval_0 \circ h_Y$, prueba que existe un único homomorfismo $h : B \longrightarrow A$ tal que $h_X = g_X \circ h$ y $h_Y = g_Y \circ h$.

$$\begin{array}{cccc} B & & & \\ & \overset{h}{\searrow} & \overset{h_X}{\searrow\searrow} & \\ {\scriptstyle h_Y}\searrow & A & \xrightarrow[g_X]{} & K[X] \\ & {\scriptstyle g_Y}\downarrow & & \downarrow{\scriptstyle eval_0} \\ & K[Y] & \xrightarrow[eval_0]{} & K \end{array}$$

SOLUCIÓN

Ejercicio. 8.21.
Dado $F \in \mathbb{C}[X]$ tal que $(F, F') = 1$, prueba que $\mathbb{C}[X]/(F)$ es un anillo reducido, esto es, sin elementos nilpotentes no nulos.

SOLUCIÓN

Ideales primos e ideales maximales

Ejercicio. 8.22.
Determina los ideales y los ideales primos del anillo $\mathbb{Z}$.

SOLUCIÓN

Ejercicio. 8.23.
Para cada entero positivo n determina los ideales y los ideales primos del anillocociente $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

SOLUCIÓN

Ejercicio. 8.24.
Demuestra que todo dominio de integridad finito D es un cuerpo.

SOLUCIÓN

Ejercicio. 8.25.
Demuestra que todo dominio de integridad D con un número finito de ideales es un cuerpo.

SOLUCIÓN

Ejercicio. 8.26.
Si $\Sigma \subseteq A$ es un subconjunto cerrado para la multiplicación que no contiene a 0, prueba que existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{m} \cap \Sigma = \varnothing$.

SOLUCIÓN

Ejercicio. 8.27.
Sea $\mathfrak{p}$ un ideal propio de un anillo A. Demuestra que son equivalentes:

(a) $\mathfrak{p}$ *es primo;*
(b) *si* $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, *entonces* $\mathfrak{a} \subseteq \mathfrak{p}$ *o* $\mathfrak{b} \subseteq \mathfrak{p}$ *para cualesquiera ideales* $\mathfrak{a}$, $\mathfrak{b}$ *de* A.

SOLUCIÓN

Ejercicio. 8.28. (AM, Cap 1, Ej 1)
Sea x un elemento nilpotente de un anillo A. Demuestra que $1 + x$ es una unidad de a. Deduce que la suma de un elemento nilpotente y una unidad es una unidad.

SOLUCIÓN

Ejercicio. 8.29. (AM, Cap 1, Ej 6)
Un anillo A es tal que cada ideal no contenido en el nilradical contiene un ***idempotente*** *no nulo (es decir, un elemento e tal que $e^2 = e \neq 0$). Demuestra que el nilradical y el radical de Jacobson de A son iguales.*

SOLUCIÓN

Ejercicio. 8.30. (AM, Cap 1, Ej 7)
Sea A un anillo en el que cada elemento x satisface $x^n = x$ para algún $n > 1$ (dependiente de x). Demuestra que cada ideal primo en A es maximal.

SOLUCIÓN

Ejercicio. 8.31. (AM, Cap 1, Ej 8)
Sea A un anillo no trivial. Demuestra que el conjunto de los ideales primos de A tiene elementos minimales respecto a la inclusión.

SOLUCIÓN

Ejercicio. 8.32. (AM, Cap 1, Ej 10)
Sea A un anillo, $\mathfrak{n}$ su nilradical. Demuestra que son equivalentes:

(a) A tiene exactamente un ideal primo.
(b) Cada elemento de A es o una unidad o nilpotente.
(c) $A/\mathfrak{n}$ es un cuerpo.

SOLUCIÓN

Ejercicio. 8.33. (AM, Cap 1, Ej 11)
Un anillo A es **anillo de Boole** *si $x^2 = x$ para cada $x \in A$. En unanillo de Boole A, demuestra que:*

(1) $2x = 0$ para todo $x \in A$.
(2) Cada ideal primo $\mathfrak{p}$ es maximal, y $A/\mathfrak{p}$ es un cuerpo con dos elementos.
(3) Cada ideal con generación finita en A es principal.

SOLUCIÓN

Ejercicio. 8.34. (AM, Cap 1, Ej 12)
Prueba que un anillo local no contiene ningún idempotente distinto de 0 y 1.

SOLUCIÓN

Ejercicio. 8.35. (AM, Cap 1, Ej 14)
En un anillo A, sea Γ el conjunto de todos los ideales en los que cada elemento es un divisor de cero.Demuestra que el conjunto Γ tiene elementos maximales y que cada elemento maximal de Γ es un ideal primo.Por tanto el conjunto de los divisores de cero en A es una unión de ideales primos.

SOLUCIÓN

Ejercicio. 8.36.
Sea D un dominio de integridad. Demuestra que si cada ideal primo no nulo es principal entonces cada ideal primo no nulo es un ideal maximal.

SOLUCIÓN

Ejercicio. 8.37.
*Sea A un anillo y $\mathfrak{a}$, $\mathfrak{b}$ ideales de A. Se define el **ideal residual** $(\mathfrak{a} : \mathfrak{b})\{x \in A \mid \; x\mathfrak{b} \subseteq \mathfrak{a}\}$.*

(1) Prueba que un ideal $\mathfrak{p}$ es primo si, y solo si, para cada ideal $\mathfrak{a}$ se tiene $(\mathfrak{p} : \mathfrak{a}) = \mathfrak{p}$ ó $(\mathfrak{p} : \mathfrak{a}) = A$.
(2) Prueba que $(n : m) = (n/d)$, donde $d = \mathrm{m.c.d.}\{n, m\}$.

SOLUCIÓN

Ejercicio. 8.38.
Sea K un cuerpo, demuestra que el ideal $(X^3 - Y^2) \subseteq K[X, Y]$ es un ideal primo del anillo $K[X, Y]$.

SOLUCIÓN

Ejercicio. 8.39.
*Un anillo A se llama **semilocal** si tiene solo un número finito de ideales maximales. Prueba que son equivalentes los siguientes enunciados:*

(a) A es un anillo semilocal.
(b) $A/\operatorname{Rad}(A)$ es un producto de cuerpos.

SOLUCIÓN

Ejercicio. 8.40.
Estudia los siguientes enunciados:

(1) Sea $p \in A$ tal que $(p) \subseteq A$ es un ideal primo. ¿Puede ser p un divisor de cero? En el caso afirmativo da una demostración, y en el negativo da un ejemplo.
(2) Plantea la misma cuestión para p nilpotente.

SOLUCIÓN

Ejercicio. 8.41.
Se consideran dos ideales principales primos no nulos (p) y (q) verificando $(p) \subseteq (q)$. Prueba que si p no es un divisor de cero entonces $(p) = (q)$.
[11, pag. 8]. SOLUCIÓN

Ejercicio. 8.42.
Estudia los siguientes enunciados:

(1) Sea $\mathfrak{p}$ un ideal primo finitamente generado con anulador cero. Prueba que $\operatorname{Ann}(\mathfrak{p}/\mathfrak{p}^2) = \mathfrak{p}$.
(2) Da un ejemplo en el se muestre que es necesario que $\mathfrak{p}$ sea primo.

[11, pag. 7] SOLUCIÓN

Ejercicio. 8.43.
Se considera $\mathfrak{p} = (p)$ un ideal primo principal de un anillo A y se define $\mathfrak{a} = \cap_{n=1}^{\infty} \mathfrak{p}^n$. Prueba los siguientes enunciados:

(1) Si $\mathfrak{q} \subsetneqq \mathfrak{p}$ es un ideal primo, entonces $\mathfrak{q} \subseteq \mathfrak{a}$.
(2) Si p no es un divisor de cero, entonces $p\,\mathfrak{a} = \mathfrak{a}$.
(3) Si p no es un divisor de cero, entonces $\mathfrak{a}$ es un ideal primo.
(4) Si A es un dominio y $\mathfrak{a}$ es finitamente generado, entonces $\mathfrak{a} = 0$ y no existen ideales primos entre 0 y $\mathfrak{p}$.
(5) Si $\mathfrak{a}$ es un ideal finitamente generado, entonces no existe una cadena de ideales primos distintos $\mathfrak{q}_2 \subsetneqq \mathfrak{q}_1 \subsetneqq \mathfrak{p}$.

[11, pag. 7–8] SOLUCIÓN

Ejercicio. 8.44.
En el anillo $\mathbb{Z}[X]$ *se considera* $\mathfrak{a} = \{F \in \mathbb{Z}[X] \mid F(0) \in 2\mathbb{Z}\}$.

(1) Prueba que $\mathfrak{a}$ *es un ideal de* $\mathbb{Z}[X]$.
(2) Prueba que $\mathfrak{a}$ *no es un ideal principal.*
(3) ¿Es $\mathfrak{a}$ *un ideal primo? ¿Es un ideal maximal?*

SOLUCIÓN

Ejercicio. 8.45.
Sea K *un cuerpo y* A *el anillo* $K[X,Y,Z]/(XY - Z^2)$. *Prueba que el ideal de* A *generado por las clases de* X *y* Z *es un ideal primo.*

SOLUCIÓN

Radical de un ideal

Ejercicio. 8.46. (AM, Cap 1, Ej 9)
Sea $\mathfrak{a}$ *un ideal propio en un anillo* A. *Demuestra que*$\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$ *si y solo si* $\mathfrak{a}$ *es una intersección de ideales primos.*

SOLUCIÓN

Ejercicio. 8.47.
Sea A *un anillo y* $\mathfrak{a}$, $\mathfrak{b}$ *ideales de* A. *Demuestra que se verifica:*

$$\mathfrak{a}^n \subseteq \mathfrak{b},\ (n \in \mathbb{N}) \Rightarrow \operatorname{rad}(\mathfrak{a}) \subseteq \operatorname{rad}(\mathfrak{b}).$$

SOLUCIÓN

Ejercicio. 8.48.
Sea $\mathfrak{a} \subseteq A$ *un ideal tal que* $\operatorname{rad}(\mathfrak{a})$ *es finitamente generado, existe* $n \in \mathbb{N}$ *tal que* $\operatorname{rad}(\mathfrak{a})^n \subseteq \mathfrak{a}$.

SOLUCIÓN

Ejercicio. 8.49.
Sea A un anillo, $\mathfrak{a}$ un ideal y $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideales primos. Si $\mathfrak{a} \subseteq \cap_{i=1}^{n}\mathfrak{p}_i \subseteq \operatorname{rad}(\mathfrak{a})$. Demuestra que $\operatorname{rad}(\mathfrak{a}) = \cap_{i=1}^{n}\mathfrak{p}_i$.

SOLUCIÓN

Ejercicio. 8.50.
Sean $\mathfrak{a}_1 = (X, Y)$, $\mathfrak{a}_2 = (X-1, Y-1)$ ideales de $\mathbb{F}_2[X, Y]$. Demuestra que $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$ es un ideal radical.

SOLUCIÓN

Ejercicio. 8.51.
Sean $\mathfrak{a}$ y $\mathfrak{b}$ ideales de un anillo A. Prueba que son equivalentes:

(a) $\mathfrak{a} + \mathfrak{b} = A$,
(b) $\operatorname{rad}(\mathfrak{a}) + \operatorname{rad}(\mathfrak{b}) = A$,

Ver Corolario (5.4.).

SOLUCIÓN

Ejercicio. 8.52.
Dados ideales $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \subseteq A$, prueba que

$$\operatorname{rad}(\mathfrak{a} + \mathfrak{b}\mathfrak{c}) = \operatorname{rad}(\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c})) = \operatorname{rad}(\mathfrak{a} + \mathfrak{b}) \cap \operatorname{rad}(\mathfrak{a} + \mathfrak{c}).$$

SOLUCIÓN

Extensión y contracción de ideales

Ejercicio. 8.53.
Sea $F : A \longrightarrow B$ un homomorfismo de anillos y $\mathfrak{a} \subseteq A$ un ideal. Demuestra que se verifica $f(\operatorname{rad}(\mathfrak{a})) \subseteq \operatorname{rad}(Bf(\mathfrak{a})) = \operatorname{rad}(\mathfrak{a}^e)$.
Si además f es sobreyectiva y $\operatorname{Ker}(f) \subseteq \mathfrak{a}$, entonces se tiene la igualdad $f(\operatorname{rad}(\mathfrak{a})) = \operatorname{rad}(Bf(\mathfrak{a}))$.

SOLUCIÓN

Ejercicio. 8.54.
Estudia los siguientes enunciados:

(1) Describe los ideales primos de $\mathbb{Z}[\sqrt{-5}]$.
(2) Considera el ideal $\mathfrak{a} = (3, 1+X) \subseteq \mathbb{Z}[X]$. *Calcula el extendido de* $\mathfrak{a}$ *en* $\mathbb{Z}[\sqrt{-5}]$.
(3) Razona que el extendido es un ideal primo que no es principal.

SOLUCIÓN

Ejercicio. 8.55.
Describe los ideales primos de $\mathbb{Z}[\sqrt{5}]$.

SOLUCIÓN

Ejercicio. 8.56.
Describe los ideales primos de $\mathbb{Z}[\sqrt{-1}]$. *Razona que todos son principales.*

SOLUCIÓN

Álgebras y anillos de polinomios

Ejercicio. 8.57. (AM, Cap 1, Ej 4)
Para cada anillo A *el radical de Jacobson de* $A[x]$ *es igual al nilradical.*

SOLUCIÓN

Ejercicio. 8.58.
Demuestra que el cuerpo $K(X)$ *de las funciones racionales en una indeterminada sobre el cuerpo* K, *esto es, el cuerpo de fracciones del anillo de polinomios* $K[X]$, *no es una* K*–álgebra finitamente generada. Observa que* $K(X)/K$ *es una extensión de cuerpos finitamente generada.*

SOLUCIÓN

Ejercicio. 8.59.
Se considera el anillo $\mathbb{Z}[X]$ *y el anillo cociente* $\mathbb{Z}[i] = \mathbb{Z}[X]/(X^2+1)$.

(1) *Razona que cada elemento de $\mathbb{Z}[i]$ tiene un único representante de la forma $a+bX$, y que con estos representantes la multiplicación está definida como*

$$(a+bX)(c+dX) = ac - bd + (ad+bc)X.$$

Podemos identificar $a+bX$ con la expresión $a+bi$, y definir la multiplicación de estas expresiones mediante la distributividad y la relación $i^2=-1$.
(2) *En $\mathbb{Z}[i]$ existe una aplicación $N:\mathbb{Z}[i]\to\mathbb{N}$, $N(a+bi)=a^2+b^2$, es la* **norma**, *y es un homomorfismo para el producto.*
(3) *Tenemos que $\mathbb{Z}[i]$ es un dominio euclídeo con aplicación euclídea la norma. Como consecuencia $\mathbb{Z}[i]$ es un DIP y un DFU.*

Se considera el homomorfismo $f:\mathbb{Z}\to\mathbb{Z}[i]$.Para cada ideal $\mathfrak{a}$ de $\mathbb{Z}[i]$ el contraído $\mathfrak{a}^c=f^{-1}(\mathfrak{a})$ es un ideal de $\mathbb{Z}$, que es primo si $\mathfrak{a}$ lo es.Para cada ideal $n\mathbb{Z}\subseteq\mathbb{Z}$, se tiene que $n\mathbb{Z}[i]$ es el extendido en $\mathbb{Z}[i]$.

(1) *Comprueba que $2\mathbb{Z}[i]$ no es un ideal primo.*
(2) *Comprueba que $3\mathbb{Z}[i]$ es un ideal primo.*
(3) *Comprueba que $5\mathbb{Z}[i]$ no es un ideal primo.*
(4) *En general, prueba que si $p\in\mathbb{Z}$ es un entero primo positivo se tiene que $p\mathbb{Z}[i]$ es un ideal primo si y solo si $p\equiv 3 \pmod 4$.*
(5) *Si $p\equiv 1 \pmod 4$ o $p=2$, entonces $p\mathbb{Z}[i]$ no es un ideal primo. Calcula en estos casos la descomposición en primos de p en $\mathbb{Z}[i]$.*

SOLUCIÓN

Ejercicio. 8.60.
Se considera un homomorfismo de anillos $f:A\to B$ y una indeterminada X. Entonces, por la propiedad universal del anillo de polinomios, existe un único homomorfismo de anillos $g:A[X]\to B[X]$ tal que $g(X)=X$ y $g_{|A}=f$.
En particular, si $\mathfrak{a}$ es un ideal de A existe un único homomorfismo, del tipo anterior, $g:A[X]\to\frac{A}{\mathfrak{a}}[X]$, que es inducido por la proyección $A\to\frac{A}{\mathfrak{a}}$.
(1) *Describe cómo está definido $g:A[X]\to\frac{A}{\mathfrak{a}}[X]$, esto es, ¿cuál es la imagen del polinomio $\sum_{i=0}^t a_iX^i$?*
(2) *Comprueba que g es sobreyectivo y calcula su núcleo.*
(3) *Describe el isomorfismo $\operatorname{Im}(g)\cong\frac{A[X]}{\operatorname{Ker}(g)}$, detallando cada uno de los anillos e ideales que en él aparecen.*
(4) *Describe $\mathbb{Z}_n[X]$ como cociente de $\mathbb{Z}[X]$.*
(5) *Describe los elementos del ideal (n) de $\mathbb{Z}[X]$*
(6) *¿Cuándo el ideal $(n)\subseteq\mathbb{Z}[X]$ es primo?*
(7) *¿Cuándo el ideal $(n)\subseteq\mathbb{Z}[X]$ es maximal?*
(8) *Da un ejemplo de un ideal maximal de $\mathbb{Z}[X]$*

SOLUCIÓN

Dominios de Factorización Única

Si D es un dominio un elemento $f \in D$ es **irreducible** si no es cero ni invertible y no tiene factorizaciones propias, esto es, si $f = gh$ en A, entonces g ó h es invertible.

Un dominio D es un **dominio de factorización única** si cada elemento no nulo ni invertible f se escribe de *forma única* como producto de elementos irreducibles.

Ejercicio. 8.61.
Prueba que para cada elemento $a \in D$ en un dominio de factorización única son equivalentes:

(a) a es irreducible.
(b) (a) es un ideal primo.

SOLUCIÓN

Ejercicio. 8.62. (AM, Cap 1, Ej 2)
Sea A un anillo y sea $A[x]$ el anillo de polinomios en una indeterminada x, con coeficientes en A. Sea $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. Demuestra que:

(1) f es una unidad en $A[x]$ si y solo si a_0 es una unidad en A y $a_1, \ldots, a_n$ con nilpotentes.
Pista. Si $b_0+b_1x+\cdots+b_mx^m$ es el inverso de f, prueba por inducción respecto de r que $a_n^{r+1}b_{m-r} = 0$. De aquí prueba que a_n es nilpotente, y entonces utiliza el ejercicio (8.28.).
(2) f es nilpotente si y solo si $a_0, a_1, \ldots, a_n$ son nilpotentes.
*(3) (**Teorema de McCoy**, 1942) f es un divisor de cero si y solo si existe $0 \neq a \in A$ tal que $af = 0$.*
Pista. Elegir un polinomio $g = b_0 + b_1x + \cdots + b_mx^m$ de grado mínimo m tal que $fg = 0$. Entonces $a_nb_m = 0$, por tanto $a_ng = 0$ (puesto que a_ng anula f y tiene grado menor que m). Después prueba por inducción que $a_{n-r}g = 0$ ($0 \leq r \leq n$).
*(4) (**Lema de Gauss**) f se dice que es **primitivo** si $(a_0, \ldots, a_n) = (1)$. Prueba que si f, $g \in A[x]$, entonces fg es primitivo si y solo si f y g son primitivos.*

SOLUCIÓN

Ejercicio. 8.63. (AM, Cap 1, Ej 3)
Generalizar los resultados del ejercicio (8.62.) a un anillo de polinomios $A[x_1, \ldots, x_n]$ de varias variables.

SOLUCIÓN

Ejercicio. 8.64. (*)
Si A es un dominio de factorización única, prueba que el anillo $A[X_1,\ldots,X_n]$ es un dominio de factorización única.

SOLUCIÓN

Ejercicio. 8.65.
Se considera el anillo $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

(1) Prueba que $\mathbb{Z}[\sqrt{-5}]$ es un dominio de integridad.
(2) Prueba que $2 \times 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ son dos factorizaciones distintas de $6 \in \mathbb{Z}\sqrt{-5}]$, y que por lo tanto $\mathbb{Z}[\sqrt{-5}]$ no es un DFU.

SOLUCIÓN

Ejercicio. 8.66.
Se considera el anillo $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

(1) Prueba que $\mathbb{Z}[\sqrt{5}]$ es un dominio de integridad.
(2) Prueba que la aplicación $N : \mathbb{Z}[\sqrt{5}] \to \mathbb{Z}$, definida $N(a+b\sqrt{5}) = a^2 - 5b^2$ es un homomorfismo para el producto.
(3) Prueba que un elemento $x \in \mathbb{Z}[\sqrt{5}]$ es invertible si y solo si $N(x) = \pm 1$.
(4) Da ejemplos de elementos $x, y \in \mathbb{Z}[\sqrt{5}]$ tales que $x \neq \pm 1$, $N(x) = 1$ y $N(y) = -1$.
(5) Prueba que si $x \in \mathbb{Z}[\sqrt{5}]$ verifica que $N(x)$ es primo en $\mathbb{Z}$, entonces x es irreducible.
(6) Prueba que la congruencia $X^2 \equiv \pm 2 \pmod 5$ no tiene soluciones en $\mathbb{Z}$, y de aquí deduce que $2, 3+\sqrt{5}, 3-\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ son irreducibles.
(7) Prueba que $4 = 2 \times 2 = (3+\sqrt{5})(3-\sqrt{5})$ son dos factorizaciones distintas de 4 en $\mathbb{Z}[\sqrt{5}]$, y que por tanto $\mathbb{Z}[\sqrt{5}]$ no es un DFU.

SOLUCIÓN

Ejercicio. 8.67.
Sea K un cuerpo y $XY - ZT \in K[X,Y,Z,T]$. Prueba que $K[X,Y,Z,T]/(XY-ZT)$

(1) es un dominio y
(2) no es un DFU.

SOLUCIÓN

Anillos de series formales de potencias

Ejercicio. 8.68.
Prueba que si D es un dominio, entonces $D[[X]]$ es un dominio, y que lo mismo ocurre con $D[[X_1,\ldots,X_n]]$.

SOLUCIÓN

Ejercicio. 8.69. (AM, Cap 1, Ej 5)
Sea A un anillo y sea $A[[X]]$ el anillo de las ***series formales de potencias*** *$f=\sum_{n=0}^{\infty}a_nX^n$ con coeficientes en A. Para cada serie formal $f=\sum_{n=0}^{\infty}a_nX^n$ se define el* ***orden*** *de f como el menor entero no negativo n tal que $a_n\neq 0$.Demuestra que:*

(1) f es una unidad en $A[[X]]$ si y solo si a_0 es una unidad en A.
(2) Si f es nilpotente, entonces a_n es nilpotente para todo $n\geq 0$. ¿Es cierto el recíproco?
(3) f pertenece al radical de Jacobson de $A[[X]]$ si y solo si a_0 pertenece al radical de Jacobson de A.
(4) La contracción de un ideal maximal $\mathfrak{m}$ de $A[[X]]$ es un ideal maximal de A, y $\mathfrak{m}$ está generado por $\mathfrak{m}^c$ y X.
(5) Cada ideal primo de A es la contracción de un ideal primo de $A[[X]]$.

SOLUCIÓN

Ejercicio. 8.70.
¿Es $7+3X+3X^2+3X^3+\cdots$ un elemento invertible en $\mathbb{Z}_{12}[[X]]$?

SOLUCIÓN

Ejercicio. 8.71.
Prueba que en $\mathbb{Z}_{12}[[X]]$ el elemento $2+3X+2X^2+3X^3+2X^4+3X^5+\cdots$ no es un divisor de cero.

SOLUCIÓN

Ejercicio. 8.72.
Sea K un cuerpo.
(1) Prueba que $(X_1,\ldots,X_n)$ es el único ideal maximal de $K[[X_1,\ldots,X_n]]$.
(2) Determina los ideales primos de $K[[X]]$.

SOLUCIÓN

Ejercicio. 8.73.
Sea A un anillo y $\mathfrak{a} \subseteq A$ un ideal.

(1) Prueba que $\mathfrak{a} + (X) \subseteq A[[X]]$ es un ideal de A.
(2) Prueba que $\mathfrak{p} \subseteq A$ es un ideal primo si, y solo si, $\mathfrak{p} + (X) \subseteq A[[X]]$ es un ideal primo.
(3) Prueba que $\mathfrak{m} \subseteq A$ es un ideal maximal si, y solo si, $\mathfrak{m} + (X) \subseteq A[[X]]$ es un ideal maximal.

SOLUCIÓN

Ejercicio. 8.74.
Sea A un anillo y $\mathfrak{a} \subseteq A$ un ideal.

(1) Prueba que $\mathfrak{a}[[X]] \subseteq A[[X]]$ es un ideal de $A[[X]]$.
(2) Prueba que $A[[X]]/\mathfrak{a}[[X]] \cong (A/\mathfrak{a})[[X]]$.
(3) Prueba que $\mathfrak{p} \subseteq A$ es un ideal primo si, y solo si, $\mathfrak{p}[[X]] \subseteq A[[X]]$ es un ideal primo.
(4) Prueba que si $\mathfrak{m} \subseteq A$ es un ideal maximal, $\mathfrak{m}[[X]] \subseteq A[[X]]$ no es maximal.

SOLUCIÓN

Ejercicio. 8.75.
Se considera el anillo $\mathbb{Q}[Y_0, Y_1, Y_2, \ldots]$, $n \in \mathbb{N}$, $n \geq 2$, el ideal $\mathfrak{a}_n = (Y_0^n, Y_1^n, Y_2^n, \ldots)$ y el anillo $A = \mathbb{Q}[Y_0, Y_1, Y_2, \ldots]/\mathfrak{a}_n$. Llamamos y_i al elemento $Y_i + \mathfrak{a}_n$ y definimos

$$F = y_0 + y_1X + y_2X^2 + \cdots \in A[[X]].$$

Prueba que F no es nilpotente, aunque cada uno de sus coeficientes es nilpotente.
(Ejemplo debido a Fields.)

SOLUCIÓN

El uso de series de potencias permite una aritmética más sencilla que la del anillo de polinomios. Ya conocemos cuando una serie de potencias es invertible. Vamos a estudiar cuando tiene una raíz cuadrada.

Ejercicio. 8.76.
Sea A un dominio. Dada $F = \sum_{i=0}^{\infty} a_iX^i \in A[[X]]$, una serie no constante de orden t.

(1) Si existe $G \in A[[X]]$ tal que $G^2 = F$, entonces t es par y a_t es un cuadrado en A.
(2) Si t es par, a_t es invertible y un cuadrado en A y 2 es invertible en A, entonces F es un cuadrado en $A[[X]]$.

Si A es un cuerpo de característica distinta de dos, las dos condiciones adicionales en (2) son ciertas y tenemos una caracterización de las series formales de potencias que tienen una raíz cuadrada.

SOLUCIÓN

Ejercicio. 8.77.
Sea $F \in \mathbb{Z}[X]$ un polinomio mónico no constante de grado par que para cada $x \in \mathbb{Z}$ se tiene $F(x)$ es un cuadrado en $\mathbb{Z}$, prueba que F es un cuadrado en $\mathbb{Z}[X]$.

SOLUCIÓN

Producto tensor de anillos

Ya conocemos el producto de dos anillos; vamos a ver que en el caso de álgebras podemos también hacer la construcción dual, esto es, el coproducto. Procedemos como sigue.

Dado un anillo A y dos A-álgebras B y C, definimos un nuevo A–módulo, $B \otimes_A C$, como el cociente del A–módulo libre sobre $\{(b,c) \mid b \in B, c \in C\}$ por el submódulo S generado por los siguientes elementos:

$$\begin{array}{llll} (b_1+b_2,c)-(b_1,c)-(b_2,c), & \forall b_1,b_2 \in B, \forall c \in C & & \\ (b,c_1+c_2)-(b,c_1)-(b,c_2), & \forall b \in B, & \forall c_1,c_2 \in C & \\ (ab,c)-(b,ac), & \forall a \in A, & \forall b \in B, & \forall c \in C \\ (ab,c)-a(b,c), & \forall a \in A, & \forall b \in B, & \forall c \in C \end{array}$$

Representamos por $b \otimes c$ a la clase en $B \otimes_A C$ del par (b,c). Por la definición los elementos de $B \otimes_A C$ son combinaciones A–lineales del tipo siguiente: $\sum_{i=1}^n b_i \otimes c_i$, con $b_i \in B$ y $c_i \in C$; es importante destacar que un elemento puede ser representado por varias expresiones distintas; por ejemplo se verifica $(b_1+b_2) \otimes c = b_1 \otimes c + b_2 \otimes c$.

Llamamos a $B \otimes_A C$ el **producto tensor** de B y C sobre A.

(Observa que hasta el momento no hemos utilizado nada más que la estructura de A–módulo de B y C, por lo que esta construcción se puede realizar para cualquier par de A–módulos.)

En el caso de dos A–álgebras, B y C, en el A–módulo $B \otimes_A C$ definimos un producto mediante:

$$(b_1 \otimes c_1)(b_2 \otimes c_2) = (b_1 b_2) \otimes (c_1 c_2), \quad \forall b_1,b_2 \in B, \forall c_1,c_2 \in C.$$

Y se extiende a todos los elementos de $B \otimes_A C$ por distributividad.

Ejercicio. 8.78.
Prueba que en $B \otimes_A C$ este producto está bien definido, esto es, que no depende de los representantes elegidos, y que $B \otimes_A C$ es una A–álgebra con elemento uno igual a $1 \otimes 1$.

SOLUCIÓN

El anillo $B \otimes_A C$ se llama el **álgebra producto tensor** de B y C sobre A.

Dados A–módulos B, C y X, una aplicación $\beta : B \times C \longrightarrow X$ se llama **A–bilineal** si verifica:

$$\begin{array}{ll} \beta(b_1 + b_2, c) = \beta(b_1, c) + \beta(b_2, c), & \forall b_1, b_2 \in B, \forall c \in C \\ \beta(b, c_1 + c_2) = \beta(b, c_1) + \beta(b, c_2), & \forall b \in B, \forall c_1, c_2 \in C \\ \beta(ab, c) = \beta(b, ac), & \forall a \in A, \forall b \in B, \forall c \in C \\ \beta(ab, c) = a\beta(b, c), & \forall a \in A, \forall b \in B, \forall c \in C \end{array}$$

Por ejemplo, siempre tenemos una aplicación A–bilineal $\tau : B \times C \longrightarrow B \otimes_A C$ definida por $\tau(b, c) = b \otimes c$, para $b \in B$ y $c \in C$.

Tenemos además que el par $(\tau, B \otimes_A C)$ verifica la siguiente propiedad universal.

Ejercicio. 8.79.

Prueba que para cada A–módulo X y cada aplicación A–bilineal $\beta : B \times C \longrightarrow X$ existe un único homomorfismo de A–módulos $\beta' : B \otimes_A C \longrightarrow X$ tal que $\beta = \beta' \circ \tau$.

$$\begin{array}{ccc} B \times C & \xrightarrow{\ \tau\ } & B \otimes_A C \\ & \searrow^{\beta} \quad \swarrow_{\beta'} & \\ & X & \end{array}$$

SOLUCIÓN

En el caso de A–álgebras también tenemos una propiedad universal. Observa que en este caso se tiene la siguiente relación con τ:

$$\tau(b_1 b_2, c_1 c_2) = \tau(b_1, c_1)\tau(b_2, c_2), \quad \forall b_1, b_2 \in B, \forall c_1, c_2 \in C;$$

por lo tanto tenemos el siguiente resultado.

Ejercicio. 8.80.

Dado un anillo A y A–álgebras B, C y X, para cada aplicación A–bilineal $\beta : B \times C \longrightarrow X$ verificando

$$\begin{array}{l} \beta(b_1 b_2, c_1 c_2) = \beta(b_1, c_1)\beta(b_2, c_2), \text{ para } b_1, b_2 \in B \text{ y } c_1, c_2 \in C, \text{ y} \\ \beta(1, 1) = 1, \end{array}$$

prueba que existe un único homomorfismo de A–álgebras $\beta' : B \otimes_A C \longrightarrow X$ tal que $\beta = \beta' \circ \tau$.

$$\begin{array}{ccc} B \times C & \xrightarrow{\ \tau\ } & B \otimes_A C \\ & \searrow^{\beta} \quad \swarrow_{\beta'} & \\ & X & \end{array}$$

SOLUCIÓN

Con estos resultados vamos a construir el dual del producto de dos A–álgebras.
Dadas dos A–álgebras B y C se definen:

$$\begin{array}{lll} j_B : B \longrightarrow B \otimes_A C, & j_B(b) = b \otimes 1, & \forall b \in B; \\ j_C : C \longrightarrow B \otimes_A C, & j_C(c) = 1 \otimes c, & \forall c \in C. \end{array}$$

Es claro que j_B y j_C son homomorfismos de A–álgebras. El resultado sobre el coproducto que andamos buscando es:

Ejercicio. 8.81.
Dada una A–álgebra X y homomorfismos de A–álgebras $f_B : B \longrightarrow X$, $f_C : C \longrightarrow X$, prueba que existe un único homomorfismo $f : B \otimes_A C \longrightarrow X$ tal que $f_B = f \circ j_B$ y $f_C = f \circ j_C$.

$$\begin{array}{ccccc} B & \xrightarrow{j_B} & B \otimes_A C & \xleftarrow{j_C} & C \\ & {\scriptstyle f_B}\searrow & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle f_C} & \\ & & X & & \end{array}$$

*Tenemos entonces que el producto tensor de dos dos anillos (conmutativos) es la **suma directa** de los mismos.*

SOLUCIÓN

Como aplicación de estos resultados hacer el siguiente:

Ejercicio. 8.82.
Dado un anillo A y dos indeterminadas X e Y, prueba que se tiene un isomorfismo de A–álgebras $A[X] \otimes_A A[X] \cong A[X,Y]$.

SOLUCIÓN

Capítulo II

Anillos de polinomios

Introducción

Este capítulo está dedicado al estudio de la aritmética de los anillos de polinomios en varias indeterminadas con coeficientes en un cuerpo. En él introducimos métodos computacionales basados en la división con resto en anillos de polinomios en n indeterminadas, para lo que necesitamos introducir relaciones de orden en $\mathbb{N}^n$, que sean un buen orden compatible con la operación suma y de forma que $0 = (0, \ldots, 0)$ sea el elemento mínimo; estos son los órdenes monomiales.

La herramienta fundamental para hacer un desarrollo computacional la proporcionan las bases de Groebner, que nos permiten diseñar algoritmos para comparar ideales y dar métodos efectivos para poder calcular las operaciones aritméticas elementales con los mismos.

9. Representación de polinomios

Se considera un cuerpo K, indeterminadas $X_1, \ldots, X_n$ y el anillo $K[X_1,\ldots,X_n]$ de los polinomios en $X_1, \ldots, X_n$ con coeficientes en K. Al identificar $K[X_1,\ldots,X_n]$ con $K[X_1,\ldots,X_{n-1}][X_n]$, cada elemento $F \in K[X_1,\ldots,X_n]$ se escribe, de forma única, como:

$$F = \sum_{i=1}^{t} F_i X_n^i, \qquad \text{con } F_i \in K[X_1,\ldots,X_{n-1}]. \tag{II.1}$$

Ésta es la **representación recursiva** de F. Sin embargo, en lo que sigue, vamos a utilizar otra representación para los polinomios en $K[X_1,\ldots,X_n]$. Dadas las indeterminadas $X_1,\ldots,X_n$, manteniendo el orden que se indica, cada producto de éstas se escribe de forma única como

$$X_1^{\alpha_1} \cdots X_n{}^{\alpha_n}.$$

Llamamos **monomio** a cada una de estas expresiones. Por simplicidad, al monomio $X_1^{\alpha_1} \cdots X_n{}^{\alpha_n}$ lo representaremos por X^α, siendo $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$. Entonces el polinomio F se puede escribir como una combinación lineal de monomios, con coeficientes en K, esto es,

$$F = \sum_{\alpha\in\mathbb{N}^n} a_\alpha X^\alpha, \qquad \text{con } a_\alpha \in K,\ \text{casi todos nulos.}$$

Ésta es la **representación distributiva** de F.

Estamos interesados en la unicidad de esta representación. Observar que aunque las expresiones $X_1X_2^5 + X_2$ y $X_2 + X_1X_2^5$ se refieren al mismo polinomio, en la práctica las consideraremos distintas, y buscaremos criterios para asociar a cada polinomio una expresión única que nos permita compararlos de forma sencilla y poder desarrollar algoritmos sobre los mismos.

10. Órdenes en $\mathbb{N}^n$

Se considera el monoide aditivo $\mathbb{N}^n$ y en él un orden (orden parcial) $\preceq$. Decimos que $\preceq$ es **compatible** o un **orden parcial lineal** si para cualesquiera $\alpha, \beta, \gamma \in \mathbb{N}^n$ tales que

$$\alpha \preceq \beta, \text{ se tiene que } \alpha + \gamma \preceq \beta + \gamma.$$

Ejemplo. 10.1. (El orden producto en $\mathbb{N}^n$)
Si consideramos en $\mathbb{N}^n$ el orden definido por

$$\alpha \leq_{pr} \beta \text{ si } \alpha_i \leq \beta_i \text{ para todo } i = 1, \ldots, n,$$

resulta que este orden es compatible.

Además, estamos interesados en órdenes totales en $\mathbb{N}^n$, y el introducido en el ejemplo anterior no lo es si $n \geq 2$.
Dado un orden total $\preceq$ en $\mathbb{N}^n$. Decimos que $\preceq$ es **monótono** o **admisible** si

$$0 = (0, \ldots, 0) \text{ es un mínimo de } \mathbb{N}^n;$$

esto es, para cada $\alpha \in \mathbb{N}^n$ se verifica $0 \preceq \alpha$. Y decimos que $\preceq$ es **fuertemente monótono** si

$$\alpha_i \leq \beta_i, \text{ para cada índice } i, \text{ entonces } (\alpha_1, \ldots, \alpha_n) \preceq (\beta_1, \ldots, \beta_n),$$

esto es, $\preceq$ es un orden que generaliza al orden producto, $\leq_{pr}$, en $\mathbb{N}^n$; ver Ejemplo (10.1.).
Es claro que todo orden fuertemente monótono es monótono. El recíproco no es siempre cierto. Sin embargo, para órdenes compatibles tenemos:

Lema. 10.2.
Todo orden compatible y monótono es fuertemente monótono.

DEMOSTRACIÓN. Supongamos que $\alpha_i \leq \beta_i$ para cada índice i, entonces existe $\gamma \in \mathbb{N}^n$ tal que $\alpha + \gamma = \beta$, como se verifica $0 \preceq \gamma$, se obtiene $\alpha \preceq \alpha + \gamma = \beta$. □

Un orden en $\mathbb{N}^n$ total, compatible y monótono se llama un **orden de términos** o un **orden monomial**.
Observa que para un **preorden** (verifica las propiedades reflexiva y transitiva) o un orden parcial en $\mathbb{N}^n$ podemos hacer también las definiciones de monótono y fuertemente monótono.

El siguiente resultado es independiente del orden total que consideremos en $\mathbb{N}^n$.

Lema. 10.3. (Lema de Dickson.)
Dado un subconjunto no vacío $S \subseteq \mathbb{N}^n$, existe un subconjunto finito $G \subseteq S$ tal que para cada $x \in S$ existen $y \in G$ y $\alpha \in \mathbb{N}^n$ tales que $x = y + \alpha$.

Se dice que G **genera** a S.

DEMOSTRACIÓN. Hacemos inducción sobre n. Si $n = 1$, entonces $S \subseteq \mathbb{N}$ y podemos tomar $G = \{y\}$, siendo y el primer elemento de S. Supongamos que $n > 1$. Tomamos $y \in S$, si existe $x \in S$ tal que $x \notin y + \mathbb{N}^n$, entonces existe un índice i tal que $x_i < y_i$, y en particular x pertenece a uno de los siguientes subconjuntos:

$$S_{ij} = \{x \in S \mid \ x_i = j\}, \quad i = 1, \ldots, n,\ j = 0, \ldots, y_i - 1.$$

Definimos nuevos subconjuntos

$$S'_{ij} = \{x \in \mathbb{N}^n \mid \ x_i = 0 \text{ y } (x_1, \ldots, x_{i-1}, j, x_{i+1}, \ldots, x_n) \in S_{ij}\}$$

Podemos considerar $S'_{ij} \subseteq \mathbb{N}^{n-1}$. Por la hipótesis de inducción, existe $G'_{ij} \subseteq S'_{ij}$ finito que genera S'_{ij}. Definimos entonces

$$G_{ij} = \{(x_1, \ldots, x_{i-1}, j, x_{i+1}, \ldots, x_n) \in S_{ij} \mid \ (x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \in G'_{ij}\}.$$

Resulta que G_{ij} es un subconjunto finito que genera S_{ij}, luego

$$\{y\} \cup (\cup_{ij} G_{ij})$$

es un conjunto finito que genera S. □

Un orden en un conjunto S es un **buen orden** si cada subconjunto no vacío tiene un primer elemento.

Ejercicio. 10.4.
Cada orden de monomial en $\mathbb{N}^n$ es un buen orden.

SOLUCIÓN. Como es un orden total, si un conjunto no vacío tiene un elemento minimal, entonces éste es único, luego es minimal. Dada una cadena $y_0 > y_1 > \cdots$ en S, consideramos el conjunto $X = \{y_0, y_1, \ldots\}$. Por el lema de Dickson existe un conjunto generador finito $\{y_{m_1}, \ldots, y_{m_t}\}$. Supongamos que $y_{m_1} \leq y_{m_i}$ para cada índice i. Si y_{m_1} no es minimal, existe $y_j < y_{m_1}$. Además existe m_i tal que $y_j = y_{m_i} + \alpha$. Como consecuencia $y_i = y_{m_i} + \alpha \geq y_{m_i} \geq y_{m_1}$, lo que es una contradicción. □

En lo que sigue vamos a trabajar, principalmente, con órdenes monomiales.

Monoideales

Un subconjunto $E \subseteq \mathbb{N}^n$ se llama un **monoideal** si para cada $\gamma \in E$ y cada $\alpha \in \mathbb{N}^n$ se tiene $\gamma + \alpha \in E$, esto es, $E = E + \mathbb{N}^n$.

Dado un monoideal E, un subconjunto $G \subseteq E$ tal que $E = G + \mathbb{N}^n$ se llama un **sistema de generadores** de E.

Como consecuencia del Lema de Dickson, Lema (10.3.), resulta que cada monoideal E de $\mathbb{N}^n$ tiene un sistema de generadores finito, esto es, E contiene un subconjunto finito G tal que $E = G + \mathbb{N}^n$.

Un sistema de generadores G de un monoideal E se llama **minimal** si ningún subconjunto de G genera E. Es fácil observar que cada monoideal contiene un sistema de generadores minimal. Sin embargo podemos decir algo más:

Lema. 10.5.
Cada monoideal tiene un único sistema de generadores minimal.

DEMOSTRACIÓN. Sea E un monoideal y G y G' dos sistemas de generadores minimales; por el Lema de Dickson podemos suponer que ambos son finitos. Para cada $\alpha \in G$ existe $\beta_\alpha \in G'$ tal que $\alpha = \beta_\alpha + \gamma_\alpha$ para algún $\gamma_\alpha \in \mathbb{N}$. Se verifica que $G_1 := \{\beta_\alpha \mid \alpha \in G\}$ genera G, y por lo tanto a G'. La minimalidad de G' se deduce que $G_1 = G'$, y por lo tanto $G' \subseteq G$. De forma análoga se tiene $G \subseteq G'$ y se tiene la igualdad. □

Órdenes en el producto cartesiano

Antes hemos hablado del orden producto en $\mathbb{N}^n$; vamos a generalizar esta construcción. Dados dos conjuntos A y B con relaciones de orden $\leq_A$ y $\leq_B$, en el producto cartesiano $A \times B$ se define una nueva relación de orden $\leq_{pr}$ mediante:

$$(a_1, b_1) \leq_{pr} (a_2, b_2) \text{ si } \begin{cases} a_1 \leq_A a_2 \text{ y} \\ b_1 \leq_B b_2 \end{cases}$$

El orden $\leq_{pr}$ se llama el **orden producto** de $\leq_A$ y $\leq_B$ en $A \times B$.

Si $\leq_A$ y $\leq_B$ son órdenes totales en A y en B respectivamente no siempre $\leq_{pr}$ es un orden total en $A \times B$, ver Ejemplo (10.1.). Por esta razón se suelen utilizar otros órdenes en $A \times B$, también inducidos por órdenes en los factores. Uno de ellos es el **orden producto lexicográfico**, que se define como

$$(a_1, b_1) \leq_{lex} (a_2, b_2) \text{ si } \begin{cases} a_1 <_A a_2 \text{ o} \\ a_1 = a_2 \text{ y } b_1 \leq_B b_2 \end{cases}$$

En este caso $\leq_{lex}$ es un orden total en $A \times B$ si $\leq_A$ y $\leq_B$ lo son.

Producto de órdenes en un conjunto

Dados dos órdenes $\preceq_1$ y $\preceq_2$ en un conjunto A, definimos un nuevo orden $\preceq$ mediante:

$$a \preceq_{1,2} b \text{ si } a \preceq_1 b \text{ y } a \preceq_2 b.$$

El orden $\preceq_{1,2}$ se llama el **orden producto** de $\preceq_1$ y $\preceq_2$. Con la notación anterior, observa que en general $\preceq_{1,2}$ y $\preceq_{2,1}$ son distintos.
Observa que si $\preceq_1$ y $\preceq_2$ son órdenes totales el orden producto $\preceq_{1,2}$ no necesariamente lo es. Este defecto lo podemos corregir cambiando la forma de definir órdenes a partir de órdenes o preórdenes dados.
Dados dos preórdenes $\sqsubseteq_1$ y $\sqsubseteq_2$ en un conjunto A, definimos un nuevo preorden en A mediante:

$$\alpha \sqsubseteq_{1,2} \beta \text{ si } \begin{cases} \alpha \sqsubset_1 \beta \text{ ó} \\ \alpha \equiv_1 \beta \text{ y } \alpha \sqsubseteq_2 \beta. \end{cases}$$

El preorden $\sqsubseteq_{1,2}$ se llama el **producto lexicográfico** de $\sqsubseteq_1$ y $\sqsubseteq_2$.

Lema. 10.6.
Con la notación anterior tenemos que $\sqsubseteq_{1,2}$ es un preorden. Además, si $\sqsubseteq_1$ y $\sqsubseteq_2$ son órdenes totales compatibles ó monótonos entonces $\sqsubseteq_{1,2}$ también lo es.

Las construcciones anteriores se puede extender a un número finito de órdenes ó preórdenes.

Ejemplos de órdenes en $\mathbb{N}^n$

Orden lexicográfico

$$\alpha \geq_{lex} \beta \text{ si para el primer índice } i \text{ tal que } \alpha_i \neq \beta_i \text{ se tiene } \alpha_i > \beta_i.$$

Orden lexicográfico graduado

$$\alpha \geq_{grlex} \beta \text{ si } \begin{cases} \sum_i \alpha_i > \sum_i \beta_i \quad \text{o} \\ \sum_i \alpha_i = \sum_i \beta_i \text{ y } \alpha \geq_{lex} \beta. \end{cases}$$

El orden $\geq_{grlex}$ es el producto lexicográfico del preorden definido por el grado y el orden lexicográfico.
Orden lexicográfico graduado inverso

$\alpha \geq_{invgrlex} \beta$ si

$$\begin{cases} \sum_i \alpha_i > \sum_i \beta_i \quad \text{o} \\ \sum_i \alpha_i = \sum_i \beta_i \text{ y para el primer índice } i \text{ (por la dcha.) tal que } \alpha_i \neq \beta_i \text{ se tiene } \alpha_i < \beta_i. \end{cases}$$

Debido a la biyección entre $\mathbb{N}^n$ y el conjunto de monomios $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, fijada una ordenación, $X_1 > X_2 > \cdots > X_n$, de las indeterminadas, dada por $(\alpha_1, \ldots, \alpha_n) \mapsto X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, cada orden o preorden en $\mathbb{N}^n$ define, de forma unívoca, un orden o preorden en el conjunto de monomios.

Ejemplo. 10.7.
Dados los monomios: X_1^3, $X_1X_2^2$, X_2^5, $X_1^3X_2X_3$, X_3^4, vamos a ordenarlos según los órdenes que hemos definido.
Orden lexicográfico: $X_1^3X_2X_3$, X_1^3, $X_1X_2^2$, X_2^5, X_3^4.
Orden lexicográfico graduado: $X_1^3X_2X_3$, X_2^5, X_3^4, X_1^3, $X_1X_2^2$.
Orden lexicográfico graduado inverso: X_2^5, $X_1^3X_2X_3$, X_3^4, X_1^3, $X_1X_2^2$.

Ejemplo. 10.8.
Ordenar los términos del polinomio $F = 3X^2 + 2XY^2 + Y^3 \in K[X, Y]$.
Orden lexicográfico:

$$F = 3X^2 + 2XY^2 + Y^3, \mathrm{lt}(F) = 3X^2, \mathrm{lc}(F) = 3, \mathrm{lm}(F) = X^2, \exp(F) = (2, 0).$$

Orden lexicográfico graduado:

$$F = 2XY^2 + Y^3 + 3X^2, \mathrm{lt}(F) = 2XY^2, \mathrm{lc}(F) = 2, \mathrm{lm}(F) = XY^2, \exp(F) = (1, 2).$$

Orden lexicográfico graduado inverso:

$$F = 2XY^2 + Y^3 + 3X^2, \mathrm{lt}(F) = 2XY^2, \mathrm{lc}(F) = 2, \mathrm{lm}(F) = XY^2, \exp(F) = (1, 2).$$

Es un resultado general que en el caso de dos indeterminadas los órdenes lexicográfico graduado y lexicográfico graduado inverso coinciden. ¡Compruébalo!

Observación. 10.9.
Observar que para aplicar estos órdenes hemos utilizado la correspondencia $X^aY^b \mapsto (a, b)$; esto supone la ordenación de las indeterminadas $X > Y$. Podríamos haber utilizado la correspondencia $X^aY^b \mapsto (b, a)$, lo que supone la ordenación de las indeterminadas en la forma $Y > X$.

11. Algoritmo de la división

Consideramos el anillo de polinomios $K[X_1,\ldots,X_n]$. Ya conocemos algo de su estructura; por ejemplo, es un dominio de factorización única. Vamos a profundiza un poco más en su aritmética.

Recordemos que como las indeterminadas se suponen conmutativas, cada producto de las mismas se puede escribir, unívocamente, en la forma $X_1^{\alpha_1}\cdots X_n^{\alpha_n}$, siendo $\alpha_i \in \mathbb{N}$, y que abreviadamente podemos representar este producto por X^α, siendo $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}^n$.

Podemos desarrollar cada polinomio $F \in K[X_1,\ldots,X_n]$ como una combinación lineal de monomios en la siguiente forma:

$$F = \sum_\alpha a_\alpha X^\alpha,$$

con $a_\alpha \in K$ (casi todos nulos), $\alpha \in \mathbb{N}^n$, y si $\alpha = (\alpha_1,\ldots,\alpha_n)$, entonces $X^\alpha = X_1^{\alpha_1}\cdots {X_n}^{\alpha_n}$.

Veamos, para fijar notación, algunos elementos asociados con el polinomio F cuando tenemos un orden monomial en $\mathbb{N}^n$.

(I) El **diagrama de Newton** de F es: $\mathcal{N}(F) = \{\alpha \in \mathbb{N}^n \mid a_\alpha \neq 0\}$.

(II) Si $F \neq 0$, el **exponente** de F: $\exp(F) = \max\{\alpha \in \mathbb{N}^n \mid \alpha \in \mathcal{N}(F)\}$.

(III) El **grado** de F: $\operatorname{grad}(F) = \max\{\alpha_1+\cdots+\alpha_n \mid \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathcal{N}(F)\}$.

(IV) El **coeficiente líder** de F: $\operatorname{lc}(F) = a_{\exp(F)}$.

(V) El **término líder** de F: $\operatorname{lt}(F) = a_{\exp(F)}X^{\exp(F)}$.

(VI) El **monomio líder** de F: $\operatorname{lm}(F) = X^{\exp(F)}$.

Por completitud definimos $\operatorname{lc}(0) = 0 = \operatorname{lt}(0)$. Como consecuencia, para cada $F \in K[X_1,\ldots,X_n]$ tenemos $F \neq 0$ si, y sólo si, $\operatorname{lt}(F) \neq 0$ si, y sólo si, $\operatorname{lc}(F) \neq 0$.

Lema. 11.1.
Dados $F,G \in K[X_1,\ldots,X_n]$ tenemos $\exp(FG) = \exp(F)+\exp(G)$.

DEMOSTRACIÓN. Como consecuencia de ser un orden compatible resulta $\exp(FG) = \exp(F) + \exp(G)$. □

De forma inmediata tenemos el siguiente resultado:

Lema. 11.2.
Dados $0 \neq F,G \in K[X_1,\ldots,X_n]$ tenemos:
(1) Si $F+G \neq 0$, entonces $\exp(F+G) \leq \max\{\exp(F),\exp(G)\}$;
(2) Si $\exp(F) < \exp(G)$, entonces $\exp(F+G) = \exp(G)$.

DEMOSTRACIÓN. □

Lo siguiente es también notación. Si $\alpha^1 \ldots, \alpha^t \in \mathbb{N}^n$, es una lista de elementos de $\mathbb{N}^n$, definimos:

$$\begin{aligned}
\Delta^1 &= \alpha^1 + \mathbb{N}^n, \\
\Delta^2 &= (\alpha^2 + \mathbb{N}^n) \setminus \Delta^1, \\
&\vdots \\
\Delta^t &= (\alpha^t + \mathbb{N}^n) \setminus \cup_{i<t} \Delta^i, \\
\overline{\Delta} &= \mathbb{N}^n \setminus \cup_{i \leq t} \Delta^i.
\end{aligned}$$

No creemos que la notación α^i para un elemento de $\mathbb{N}^n$ se confunda con la *i*–ésima potencia de α, ya que no vamos a usar potencias de elementos de $\mathbb{N}^n$ a lo largo de este trabajo.

Lema. 11.3.
Para cada lista de elementos de $\mathbb{N}^n$, por ejemplo $\alpha^1, \ldots, \alpha^t$, tenemos que $\{\Delta^1, \Delta^2, \ldots, \Delta^t, \overline{\Delta}\}$ es una partición de $\mathbb{N}^n$, cuando eliminamos los conjuntos vacíos.

DEMOSTRACIÓN. □

Una consecuencia de este resultado es el siguiente algoritmo de la división en el anillo $K[X_1, \ldots, X_n]$.

Teorema. 11.4. (Algoritmo de la división)
Dado un orden monomial en $\mathbb{N}^n$, para cada lista finita de polinomios no nulos

$$G_1, \ldots, G_t \in K[X_1, \ldots, X_n],$$

consideramos la partición de $\mathbb{N}^n$ determinada por la lista

$$\exp(G_1), \ldots, \exp(G_t).$$

Se verifica que para cada $0 \neq F \in K[X_1, \ldots, X_n]$ existen elementos $Q_1, \ldots, Q_t$ y $R \in K[X_1, \ldots, X_n]$, únicos, cumpliendo las propiedades siguientes:
(1) $F = \sum_{i=1}^{t} Q_i G_i + R$.
(2) $R = 0$ *ó* $\mathcal{N}(R) \subseteq \overline{\Delta}$.
(3) Para cada índice i se verifica: $\exp(G_i) + \mathcal{N}(Q_i) \subseteq \Delta^i$.

Como consecuencia, si $Q_i G_i \neq 0$, se tiene $\exp(Q_i G_i) \leq \exp(F)$ y si $R \neq 0$, entonces $\exp(R) \leq \exp(F)$.

DEMOSTRACIÓN.
Existencia.
Hacemos inducción sobre $\exp(F)$. Si $\exp(F) = 0$, entonces tenemos dos posibilidades:

(I) $\exp(F) = (0,\dots,0) \in \Delta^i$, para algún índice i.

(II) $\exp(F) = (0,\dots,0) \in \overline{\Delta}$.

(i) Tenemos $\exp(F) = \exp(G_i) + \gamma$, para algún $\gamma \in \mathbb{N}^n$, luego $\exp(G_i) = (0,\dots,0)$ y $G_i \in K$. Podemos tomar:

$$\begin{cases} Q_j = 0, & \text{si } j \neq i; \\ Q_i = F_i/G_i; \\ R = 0 \end{cases}$$

(ii) Tenemos $\exp(F) \in \overline{\Delta}$, entonces podemos tomar:

$$\begin{cases} Q_i = 0, & \text{si } i = 1,\dots,t; \\ R = F \end{cases}$$

Supongamos ahora que el resultado es cierto para todos los polinomios G con $\exp(G) < \exp(F)$. Al igual que antes tenemos dos posibilidades:

(I) $\exp(F) \in \Delta^i$, para algún índice i;

(II) $\exp(F) \in \overline{\Delta}$.

(i) Tenemos $\exp(F) = \exp(G_i) + \gamma$, para algún $\gamma \in \mathbb{N}^n$. Si definimos $H = X^\gamma G_i$ tenemos que $F - \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma G_i$ es un polinomio con exponente estrictamente menor que F. Aplicando la hipótesis de inducción tenemos:

$$F - \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma G_i = \sum_i Q'_i G_i + R'$$

con los $Q'_1,\dots,Q'_t, R$ verificando las condiciones del enunciado. Entonces obtenemos la expresión:

$$F = \sum_i Q_i G_i + R,$$

en donde

$$\begin{cases} Q_j = Q'_j, & \text{si } j \neq i; \\ Q_i = Q'_i + \frac{\mathrm{lc}(F)}{\mathrm{lc}(H)} X^\gamma; \\ R = R' \end{cases}$$

Para comprobar que se tienen las condiciones del enunciado observemos las siguientes inclusiones:

$$\begin{aligned} \exp(G_i) + \mathcal{N}(Q_i) &\subseteq \exp(G_i) + \{\mathcal{N}(Q'_i) \cup \{\gamma\}\} = \\ &= (\exp(G_i) + \mathcal{N}(Q'_i)) \cup \{\exp(G_i) + \gamma\} \subseteq \\ &\subseteq \Delta^i. \end{aligned}$$

(ii) Si $\exp(F) \in \overline{\Delta}$, entonces $F - \mathrm{lt}(F)$ es un polinomio con exponente estrictamente menor que F, y por tanto, por la hipótesis de inducción, tenemos:

$$F - \mathrm{lt}(F) = \sum_i Q'_i G_i + R'$$

con los $Q'_1, \ldots, Q'_t, R$ verificando las condiciones del enunciado. Entonces obtenemos la siguiente expresión para F:

$$F = \sum_i Q_i G_i + R,$$

en donde

$$\begin{cases} Q_i = Q'_i, & \text{si } i = 1, \ldots, t; \\ R = R' + \operatorname{lt}(F) \end{cases}$$

Para comprobar que se tienen las condiciones del enunciado tenemos que si $R \neq 0$, entonces, considerando que $\mathcal{N}(0) = \varnothing$, tenemos:

$$\mathcal{N}(R) = \mathcal{N}(R' + \operatorname{lt}(F)) \subseteq \mathcal{N}(R') \cup \{\exp(F)\} \subseteq \overline{\Delta}.$$

Unicidad.
Sean

$$F = \sum_i Q_i G_i + R = \sum_i Q'_i G_i + R'$$

dos expresiones de F verificando las condiciones del enunciado. Tenemos entonces:

$$0 = \sum_i (Q_i - Q'_i) G_i + (R - R').$$

Vamos a analizar los exponentes de los sumandos de esta suma:

$$\exp(R - R') \in \mathcal{N}(R - R') \subseteq \mathcal{N}(R) \cup \mathcal{N}(R') \subseteq \overline{\Delta}.$$

$$\begin{aligned} \exp((Q_i - Q'_i)G_i) &= \exp(Q_i - Q'_i) + \exp(G_i) \subseteq \\ &\subseteq \exp(G_i) + (\mathcal{N}(Q_i - Q'_i)) = \\ &= (\exp(G_i) + \mathcal{N}(Q_i)) \cup (\exp(G_i) + \mathcal{N}(Q'_i)) \\ &\subseteq \Delta^i. \end{aligned}$$

Ahora como los $\Delta^1, \ldots, \Delta^t, \overline{\Delta}$ forman una partición de $\mathbb{N}^n$, llegamos a que cada uno de los sumandos es cero, y como estamos en un dominio, tenemos $Q_i = Q'_i$, para cada índice i, y $R = R'$. □

Los $Q_1, \ldots, Q_t$ se llaman los **cocientes** de F y R se llama el **resto** de F relativos a $\{G_1, \ldots, G_t\}$. El resto R se representa también por $R(F; \{G_1, \ldots, G_t\})$.
Observa que el orden de los elementos $G_1, \ldots, G_t$ es determinante para el cálculo del resto. Esto es, puede ocurrir que:

$$R(F; \{G_1, \ldots, G_i, \ldots, G_j, \ldots, G_t\}) \neq R(F; \{G_1, \ldots, G_j, \ldots, G_i, \ldots, G_t\}),$$

cuando $i \neq j$.

Ejercicio. 11.5.
Se consideran los polinomios $F, G_1, G_2, G_3 \in \mathbb{Q}[X, Y, Z]$.

$$\begin{aligned} F &= X^4Y^2 + X^2Y^3Z - 2XY^2Z^3 - 3X^2YZ^4, \\ G_1 &= X^3Y - 2X^2Z^2, \\ G_2 &= X^2Y^3 + XZ^3, \\ G_3 &= XY^2Z - X^2YZ - 3XYZ^2. \end{aligned}$$

Con respecto al orden lexicográfico haz la división de F *por* $\{G_1, G_2, G_3\}$ *y la división de* F *por* $\{G_3, G_2, G_1\}$. *Comprueba que son distintas.*

SOLUCIÓN. Sean

$$\begin{aligned} F &= X^4Y^2 + X^2Y^3Z - 2XY^2Z^3 - 3X^2YZ^4, \\ G_1 &= X^3Y - 2X^2Z^2, \\ G_2 &= X^2Y^3 + XZ^3, \\ G_3 &= XY^2Z - X^2YZ - 3XYZ^2. \end{aligned}$$

para hacer la división de F por $\{G_1, G_2, G_3\}$ consideramos la siguiente tabla:

$\Delta^1 =$	$(3,1,0) + \mathbb{N}^3$						
$\Delta^2 =$	$((2,3,0) + \mathbb{N}^3) \setminus \Delta^1$						
$\Delta^3 =$	$((2,1,1) + \mathbb{N}^3) \setminus \Delta^2$						
i	F_i	$\exp(F_i)$	$\in$	Q_1	Q_2	Q_3	R
0	$X^4Y^2 + X^2Y^3Z - 2XY^2Z^3 - 3X^2YZ^4$	$(4,2,0)$	Δ^1	XY			
1	$X^2Y^3Z + 2X^3YZ^2 - 2XY^2Z^3 - 3X^2YZ^4$	$(3,1,2)$	Δ^1	$2Z^2$			
2	$X^2Y^3Z - 2XY^2Z^3 + 4X^2Z^4 - 3X^2YZ^4$	$(2,3,1)$	Δ^2		Z		
3	$-2XY^2Z^3 - XZ^4 + 4X^2Z^4 - 3X^2YZ^4$	$(2,1,4)$	Δ^3			$3Z^3$	
4	$-2XY^2Z^3 - XZ^4 + 4X^2Z^4 - 3XY^2Z^4 + 9XYZ^5$	$(2,0,4)$	$\overline{\Delta}$				$4X^2Z^4$
5	$-2XY^2Z^3 - XZ^4 - 3XY^2Z^4 + 9XYZ^5$	$(1,2,4)$	$\overline{\Delta}$				$-3XY^2Z^4$
6	$-2XY^2Z^3 - XZ^4 + 9XYZ^5$	$(1,2,3)$	$\overline{\Delta}$				$-2XY^2Z^3$
7	$-XZ^4 + 9XYZ^5$	$(1,1,5)$	$\overline{\Delta}$				$9XYZ^5$
8	$-XZ^4$	$(1,0,4)$	$\overline{\Delta}$				$-XZ^4$
$\sum$	0			$XY + 2Z^2$	Z	$3Z^3$	$--$

$$F = (XY + 2Z^2)G_1 + ZG_2 + (3Z^3)G_3 + (4X^2Z^4 - 3XY^2Z^4 - 2XY^2Z^3 + 9XYZ^5 - XZ^4).$$

En el caso de la división de F por $\{G_3, G_2, G_1\}$, el resultado es:

$$F = (-2XZ - Y^2 - 2YZ + 3Z^3 + 6Z^2)G_3 + 0G_2 + (XY)G_1 + (XY^4Z - XY^3Z^2 - 3XY^2Z^4 - 14XY^2Z^3 + 9XYZ^5 + 18XYZ^4).$$

□

12. Ideales monomiales

Un ideal $\mathfrak{a}$ de $K[X_1,\ldots,X_n]$ se llama **monomial** si tiene un sistema de generadores formado por monomios. El resultado fundamental de esta sección es que los ideales monomiales de $K[X_1,\ldots,X_n]$ se pueden estudiar a través de los monoideales de $\mathbb{N}^n$.

Lema. 12.1.
Si $\mathfrak{a}$ es un ideal monomial con un sistema de generadores formado por monomios $\{X^\alpha \mid \alpha \in A \subseteq \mathbb{N}^n\}$, para cada monomio $X^\beta \in K[X_1,\ldots,X_n]$ son equivalentes:
(a) $X^\beta \in \mathfrak{a}$.
(b) Existe $F \in K[X_1,\ldots,X_n]$ tal que $X^\beta = FX^\alpha$, para algún $\alpha \in A$.

Además, este F se puede tomar monomial.

DEMOSTRACIÓN. Es claro que (b) implica (a). Para ver que (a) implica (b), sea $\{X^\alpha \mid \alpha \in A\}$ un sistema de generadores de $\mathfrak{a}$ formado por monomios, y sea $X^\beta \in \mathfrak{a}$. Entonces existen $F_1, \ldots, F_t \in K[X_1,\ldots,X_n]$ y $\alpha^1,\ldots,\alpha^t \in A$ tales que $X^\beta = \sum_i F_i X^{\alpha^i}$. Supongamos que $F_i = \sum_j b_{ij} X^{\beta^{ij}}$, con $b_{ij} \in K$, tenemos la expresión siguiente:

$$X^\beta = \sum_i F_i X^{\alpha^i} = \sum_i \left(\sum_j b_{ij} X^{\beta^{ij}} \right) X^{\alpha^i} = \sum_{i,j} b_{ij} X^{\beta^{ij}} X^{\alpha^i} = \sum_{i,j} d_{ij} X^{\alpha^i + \beta^{ij}}.$$

Los monomios unitarios son una K–base de $K[X_1,\ldots,X_n]$, luego de $X^\beta = \sum_{i,j} d_{ij} X^{\alpha^i+\beta^{ij}}$ deducimos que la expresión anterior se puede escribir

$$X^\beta = \left(\sum \{ d_{ij} \mid \alpha^i + \beta^{ij} = \beta \} \right) X^\beta,$$

y como consecuencia, para algún α^i se tiene que existe un γ tal que $\alpha^i + \gamma = \beta$, entonces existe un $c \in K$ tal que $X^\beta = cX^\gamma X^{\alpha^i}$, de donde se tiene el resultado. □

Proposición. 12.2.
Sea $\mathfrak{a}$ un ideal monomial y sea F un elemento de $K[X_1,\ldots,X_n]$. Son equivalentes los siguientes enunciados:
(a) $F \in \mathfrak{a}$.
(b) Todo monomio de F pertenece a $\mathfrak{a}$.
(c) F es una combinación K–lineal de monomios de $\mathfrak{a}$.

DEMOSTRACIÓN. Las relaciones (b) $\Leftrightarrow$ (c) $\Rightarrow$ (a) son claras. Para probar que (a) implica (b), consideremos $\{X^\alpha \mid \alpha \in A\}$ un sistema de generadores de $\mathfrak{a}$ formado por monomios para algún conjunto A. Sea $F \in \mathfrak{a}$, existen $F_1, \ldots, F_t \in K[X_1, \ldots, X_n]$ y $\alpha^1, \ldots, \alpha^t \in A$ tales que $F = \sum_i F_i X^{\alpha^i}$. Consideramos desarrollos de los F_i, por ejemplo, $F_i = \sum_j b_{ij} X^{\beta^{ij}}$, con $b_{ij} \in K$. Tenemos la expresión siguiente:

$$\begin{aligned} F = & \sum_i F_i X^{\alpha^i} = \\ & = \sum_i (\sum_j b_{ij} X^{\beta^{ij}}) X^{\alpha^i} = \\ & = \sum_{i,j} b_{ij} X^{\beta^{ij}} X^{\alpha^i} = \\ & = \sum_{i,j} d_{ij} X^{\alpha^i + \beta^{ij}} = \\ & = \sum_\beta c_\beta X^\beta . \end{aligned}$$

Si algún $c_\beta \neq 0$, entonces $0 \neq c_\beta = \sum\{d_{ij} \mid \alpha^i + \beta^{ij} = \beta\}$, y al igual que en la demostración del lema anterior tenemos que existe algún $\alpha^i \in A$ y algún $c \in K$ tales que

$$c_\beta X^\beta = c X^\gamma X^{\alpha^i},$$

de donde cada monomio de F pertenece a $\mathfrak{a}$. □

Si $\mathfrak{a}$ es un ideal definimos

$$\mathrm{Exp}(\mathfrak{a}) = \{\exp(F) \mid 0 \neq F \in \mathfrak{a}\}.$$

Un subconjunto $E \subseteq \mathbb{N}^n$ se llama un **monoideal**, ver página 61, si para cada $\gamma \in E$ y cada $\alpha \in \mathbb{N}^n$ se tiene $\gamma + \alpha \in E$, esto es, si $E = E + \mathbb{N}^n$.

Lema. 12.3.
Para cada ideal $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ se tiene que $\mathrm{Exp}(\mathfrak{a})$ es un monoideal de $\mathbb{N}^n$.

Corolario. 12.4. (Lema de Dickson para ideales monomiales)
Si $\mathfrak{a}$ es un ideal monomial, entonces $\mathfrak{a}$ tiene un sistema finito de generadores formado por monomios.

DEMOSTRACIÓN. Como tenemos que $\mathrm{Exp}(\mathfrak{a})$ es un monoideal de $\mathbb{N}^n$, sea $A \subseteq \mathrm{Exp}(\mathfrak{a})$ finito tal que $\mathrm{Exp}(\mathfrak{a}) = A + \mathbb{N}^n$. Para cada $\alpha \in A$ consideramos $F_\alpha \in \mathfrak{a}$ tal que $\exp(F_\alpha) = \alpha$. Es claro que $\mathrm{lm}(F_\alpha) = \mathrm{lc}(F_\alpha) X^\alpha$, luego $X^\alpha \in \mathfrak{a}$. Consideramos ahora el ideal $\mathfrak{b} = R(\{X^\alpha \mid \alpha \in A\})$. Se verifica que $\mathfrak{b} \subseteq \mathfrak{a}$. Además, dado un monomio $X^\beta \in \mathfrak{a}$ tenemos $\beta \in \mathrm{Exp}(\mathfrak{a}) = A + \mathbb{N}^n$, luego existe $\alpha \in A$ y $\gamma \in \mathbb{N}^n$ tales que $\beta = \alpha + \gamma$. Entonces tenemos:

$$X^\beta = X^{\alpha+\gamma} = c X^\gamma X^\alpha,$$

para algún $c \in K$, y por tanto $X^\beta \in \mathfrak{b}$. □

Una demostración directa de este resultado aparece en los ejercicios.

Como consecuencia de la demostración del Lema de Dickson para ideales monomiales tenemos:

Corolario. 12.5.
Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales monomiales, son equivalentes los siguientes enunciados:

(a) $\mathfrak{a} = \mathfrak{b}$*;*
(b) $\operatorname{Exp}(\mathfrak{a}) = \operatorname{Exp}(\mathfrak{b})$.

El siguiente resultado es de interés, ya que en teoría permite comparar ideales monomiales.

Proposición. 12.6.
Cada ideal monomial tiene un (único) sistema finito mínimo de generadores.

DEMOSTRACIÓN. Sean G y G' dos sistemas de generadores. Para cada $g \in G$ existe $g' \in G'$ tal que $g' \mid g$, luego $G \setminus \{g\} \cup \{g'\}$ es un nuevo sistema de generadores que ocupa el lugar de G. Si realizamos este proceso para cada sistema de generadores G', llegamos a un sistema de generadores mínimo. □

Es claro que existe una biyección entre ideales monomiales de $K[X_1, \ldots, X_n]$ y monoideales de $\mathbb{N}^n$. En esta biyección a cada ideal $\mathfrak{a}$ le corresponde el monoideal $\operatorname{Exp}(\mathfrak{a})$, y a cada monoideal $E \subseteq \mathbb{N}^n$, con sistema de generadores G le corresponde el ideal monomial con sistema de generadores $\{X^\gamma \mid \gamma \in G\}$. En ambos casos los sistemas de generadores pueden ser tomados finitos.

13. Bases de Groebner

Vamos a tratar ahora el caso general de un ideal no nulo del anillo de polinomios y vamos a ver si es posible obtener un sistema de generadores que sea mínimo en algún sentido.

Lema. 13.1.
Sea $\mathfrak{a}$ un ideal no nulo de $K[X_1,\ldots,X_n]$. Si $A \subseteq \mathbb{N}^n$ es un sistema finito de generadores de $\operatorname{Exp}(\mathfrak{a})$, para cada conjunto de polinomios $\{F_\alpha \mid \alpha \in A\} \subseteq \mathfrak{a}$ tales que $\exp(F_\alpha) = \alpha$ para cada $\alpha \in A$, se tiene que $\{F_\alpha \mid \alpha \in A\}$ es sistema de generadores de $\mathfrak{a}$ como ideal.

DEMOSTRACIÓN. Como A es finito, supongamos que $\{F_\alpha \mid \alpha \in A\} = \{G_1,\ldots,G_t\}$. Para cada $0 \neq F \in \mathfrak{a}$ consideramos el algoritmo de la división para la sucesión $G_1,\ldots,G_t$. Obtenemos una expresión $F = \sum_i Q_iG_i + R$. Si $R \neq 0$, entonces $\mathcal{N}(R) \subseteq \overline{\Delta}$ y como tenemos $R = F - \sum_i Q_iG_i \in \mathfrak{a}$, se verifica $\exp(R) \in \operatorname{Exp}(\mathfrak{a}) = A + \mathbb{N}^n = \cup_i\Delta^i$, lo que es una contradicción. □

Si $\mathfrak{a}$ es un ideal de $K[X_1,\ldots,X_n]$, una **base de Groebner** de $\mathfrak{a}$ es un conjunto finito de elementos no nulos, $\mathbb{G} = \{G_1,\ldots,G_t\} \subseteq \mathfrak{a}$, verificando que

$$\operatorname{Exp}(\mathfrak{a}) = \{\exp(G_1),\ldots,\exp(G_t)\} + \mathbb{N}^n = \operatorname{Exp}(\mathbb{G}) + \mathbb{N}^n.$$

Corolario. 13.2.
(1) Cada ideal no nulo de $K[X_1,\ldots,X_n]$ tiene una base de Groebner.
(2) Toda base de Groebner de un ideal no nulo es un sistema de generadores.
*(3) **Teorema de la base de Hilbert.** Todo ideal de $K[X_1,\ldots,X_n]$ es finitamente generado.*

Proposición. 13.3.
Dados $\mathfrak{a}$ es un ideal no nulo de $K[X_1,\ldots,X_n]$, y $\mathbb{G}$, $\mathbb{G}'$ son dos bases de Groebner de $\mathfrak{a}$, para cada $0 \neq F \in K[X_1,\ldots,X_n]$ se verifica $R(F;\mathbb{G}) = R(F;\mathbb{G}')$.

DEMOSTRACIÓN. Supongamos que al aplicar el algoritmo de la división para $\mathbb{G}$ y $\mathbb{G}'$ obtenemos dos expresiones:

$$F = \sum_i Q_iG_i + R = \sum_j Q'_jG'_j + R',$$

respectivamente. Si $R \neq R'$, como $R - R' \in \mathfrak{a}$, tenemos

$$\exp(R-R') \in \operatorname{Exp}(\mathfrak{a}) = \cup_i\Delta^i = \cup_j(\Delta')^j.$$

Pero

$$\exp(R-R') \in \mathcal{N}(R-R') \subseteq \mathcal{N}(R) \cup \mathcal{N}(R') \subseteq \overline{\Delta} = \overline{\Delta'} = \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a}),$$

lo que es una contradicción. □

Algoritmo de Buchberger

Se trata ahora de caracterizar las bases de Groebner para después dar un algoritmo que permita calcular una de ellas.

Proposición. 13.4.
Sea $\mathfrak{a}$ un ideal no nulo de $K[X_1,\ldots,X_n]$ y $\mathbb{G}$ una familia finita de elementos de $\mathfrak{a}$. Son equivalentes los siguientes enunciados:

(a) $\mathbb{G}$ es una base de Groebner de $\mathfrak{a}$.
(b) Para cada $0 \neq F \in \mathfrak{a}$ se tiene $R(F;\mathbb{G}) = 0$.

DEMOSTRACIÓN. (a)⇒(b). Si $R(F;\mathbb{G}) \neq 0$, entonces $\exp(R(F;\mathbb{G})) \in \operatorname{Exp}(\mathfrak{a}) \cap \overline{\Delta} = \varnothing$, lo que es una contradicción.
(b)⇒(a). Sea $0 \neq F \in \mathfrak{a}$, por el algoritmo de la división existen $Q_1,\ldots,Q_t, R \in K[X_1,\ldots,X_n]$ tales que:

$$F = \sum_i Q_iG_i, \qquad \text{y} \qquad \exp(G_i) + \mathcal{N}(Q_i) \subseteq \Delta^i.$$

En consecuencia, $\exp(Q_iG_i) \neq \exp(Q_jG_j)$ si $i \neq j$, y $\exp(F)$ es el máximo de los exponentes de los sumandos Q_iG_i. Existe un índice i tal que

$$\exp(F) = \exp(Q_iG_i) \in \Delta^i \subseteq \exp(G_i) + \mathbb{N}^n,$$

y por tanto $\exp(F) \in \{\exp(G_1),\ldots,\exp(G_t)\} + \mathbb{N}^n$. □

Esta caracterización de las bases de Groebner no es muy práctica, ya que habría que probar con todos los elementos del ideal $\mathfrak{a}$ para ver que tenemos una base de Groebner. Se trata entonces de buscar criterios más prácticos para caracterizar bases de Groebner.
Vamos a introducir en este punto la notación necesaria para su desarrollo.
Si X^α y X^β son dos monomios, vamos a definir su mínimo común múltiplo. Definimos:

$$\gamma_i = \max\{\alpha_i, \beta_i\}, \qquad 1 \leq i \leq n.$$

Sea $\gamma = (\gamma_1,\ldots,\gamma_n) \in \mathbb{N}^n$, entonces llamamos a X^γ el **mínimo común múltiplo** de X^α y X^β. Tenemos que X^γ es realmente un múltiplo ya que se verifica:

$$X^\gamma = X^{\gamma-\alpha}X^\alpha.$$

Y el resultado análogo para X^β:

$$X^\gamma = X^{\gamma-\beta}X^\beta.$$

El mínimo común múltiplo se representa por $\operatorname{m.c.m.}\{X^\alpha, X^\beta\}$.

Con este bagaje vamos a definir las **semisicigias** ó **s–polinomios**. Dados $F,G \in K[X_1,\dots,X_n]$, con $\exp(F)=\alpha$ y $\exp(G)=\beta$, el s–polinomio definido por F y G es:

$$S(F,G)=\frac{1}{\mathrm{lc}(F)}X^{\gamma-\alpha}F-\frac{1}{\mathrm{lc}(G)}X^{\gamma-\beta}G.$$

Lema. 13.5. (Lema técnico)
Se considera la expresión $\sum_{i=1}^{t} c_iX^{\alpha^i}F_i$, en donde: los F_i son elementos de $K[X_1,\dots,X_n]$, $c_i \in K$ y $\alpha^i \in \mathbb{N}^n$, verificando:

$$\exp(\sum_i c_iX^{\alpha^i}F_i)<\delta=\exp(X^{\alpha^i}F_i),\ \text{para cada índice } i.$$

Entonces existen elementos $c_{jk}\in K$ tales que:

$$\sum_i c_iX^{\alpha^i}F_i=\sum_{jk} c_{jk}X^{\delta-\gamma^{jk}}S(F_j,F_k),\quad y\quad \exp(X^{\delta-\gamma^{jk}}S(F_j,F_k))<\delta,$$

en donde $X^{\gamma^{jk}}=\mathrm{m.c.m.}\{X^{\exp(F_j)},X^{\exp(F_k)}\}$.

DEMOSTRACIÓN. Supongamos que $\exp(F_i)=\beta^i$, entonces $\alpha^i+\beta^i=\delta$. Hacemos el siguiente desarrollo:

$$\sum_i c_iX^{\alpha^i}F_i=\sum_i c_i\,\mathrm{lc}(F_i)\frac{X^{\alpha^i}F_i}{\mathrm{lc}(F_i)}=\sum_i c_i\,\mathrm{lc}(F_i)H_i,$$

donde $\frac{X^{\alpha^i}F_i}{\mathrm{lc}(F_i)}=H_i$ Podemos completar este desarrollo de la siguiente forma:

$$\sum_i c_iX^{\alpha^i}F_i=\sum_i c_i\,\mathrm{lc}(F_i)H_i=$$

$$=c_1\,\mathrm{lc}(F_1)(H_1-H_2)+(c_1\,\mathrm{lc}(F_1)+c_2\,\mathrm{lc}(F_2))(H_2-H_3)+\cdots$$
$$\cdots+(c_1\,\mathrm{lc}(F_1)+\cdots+c_{t-1}\,\mathrm{lc}(F_{t-1}))(H_{t-1}-H_t)+$$
$$+(c_1\,\mathrm{lc}(F_1)+\cdots+c_t\,\mathrm{lc}(F_t))H_t.$$

Consideramos ahora el producto $X^{\delta-\gamma^{jk}}S(F_j,F_k)$. Vamos a desarrollarlo y ver que vamos a obtener un múltiplo de H_j-H_k.

$$X^{\delta-\gamma^{jk}}S(F_j,F_k)=$$
$$=X^{\delta-\gamma^{jk}}\left(\frac{1}{\mathrm{lc}(F_j)}X^{\gamma^{jk}-\beta^j}F_j-\frac{1}{\mathrm{lc}(F_k)}X^{\gamma^{jk}-\beta^k}F_k\right)=$$

$$= \frac{1}{\operatorname{lc}(F_j)} X^{\delta-\gamma^{jk}} X^{\gamma^{jk}-\beta^j} F_j - \frac{1}{\operatorname{lc}(F_k)} X^{\delta-\gamma^{jk}} X^{\gamma^{jk}-\beta^k} F_k =$$
$$= \frac{1}{\operatorname{lc}(F_j)} X^{\delta-\beta^j} F_j - \frac{1}{\operatorname{lc}(F_k)} X^{\delta-\beta^k} F_k =$$
$$= \frac{1}{\operatorname{lc}(F_j)} X^{\delta-\beta^j} F_j - \frac{1}{\operatorname{lc}(F_k)} X^{\delta-\beta^k} F_k =$$
$$= \frac{X^{\alpha^j} F_j}{\operatorname{lc}(F_j)} - \frac{X^{\alpha^k} F_k}{\operatorname{lc}(F_k)} =$$
$$= H_j - H_k.$$

Entonces tenemos

$$X^{\delta-\gamma^{jk}} S(F_j, F_k) = H_j - H_k.$$

Ahora como $\sum_i c_i \operatorname{lc}(F_i) = 0$, tenemos:

$$\sum c_i X^{\alpha^i} F_i =$$
$$c_1 \operatorname{lc}(F_1) X^{\delta-\gamma^{12}} S(F_1, F_2) +$$
$$+ (c_1 \operatorname{lc}(F_1) + c_2 \operatorname{lc}(F_2)) X^{\delta-\gamma^{23}} S(F_2, F_3) + \cdots$$
$$\cdots + (c_1 \operatorname{lc}(F_1) + \cdots + c_{t-1} \operatorname{lc}(F_{t-1}))$$
$$X^{\delta-\gamma^{t-1,t}} S(F_{t-1}, F_t).$$

Y tenemos la primera parte del enunciado. Para la segunda parte tenemos en cuenta que cada H_i es un polinomio mónico con $\exp(H_i) = \delta$, entonces $\exp(H_i - H_j) < \delta$ y tenemos el resultado. □

Teorema. 13.6. (Teorema de Buchberger)
Sea $\mathfrak{a}$ un ideal no nulo del anillo $K[X_1, \ldots, X_n]$ y $\mathbb{G}$ un sistema finito de generadores de $\mathfrak{a}$. Son equivalentes los siguientes enunciados:

(a) $\mathbb{G}$ es una base de Groebner de $\mathfrak{a}$.
(b) Para un orden fijado de $\mathbb{G}$ y para cada $i \neq j$ se tiene $R(S(G_i, G_j); \mathbb{G}) = 0$.

DEMOSTRACIÓN. (a)⇒(b). Es evidente.
(b)⇒(a). Sea $0 \neq F \in \mathfrak{a}$, entonces $F = \sum Q_i G_i$ y tenemos

$$\exp(F) \leq \max\{\exp(Q_i G_i) \mid i = 1, \ldots, t\}.$$

Vamos a ver que podemos alcanzar la igualdad. Llamamos:

$$\delta = \max\{\exp(Q_i G_i) \mid i = 1, \ldots, t\},$$
$$\delta^i = \exp(Q_i G_i).$$

Si $\exp(F) < \delta$, descomponemos F en la siguiente forma:

$$\begin{aligned} F &= \sum_i Q_iG_i = \\ &= \sum_{\delta^i=\delta} Q_iG_i + \sum_{\delta^i<\delta} Q_iG_i = \\ &= \sum_{\delta^i=\delta} \operatorname{lm}(Q_i)G_i + \sum_{\delta^i=\delta}(Q_i - \operatorname{lm}(Q_i))G_i + \sum_{\delta^i<\delta} Q_iG_i. \end{aligned}$$

las dos últimas sumas son "*despreciables*", ya que su exponente es menor que δ. Vamos a cambiar $\sum_{\delta^i=\delta} \operatorname{lm}(Q_i)G_i$ mediante otra expresión. Usando el Lema (13.5.) tenemos:

$$\sum_{\delta^i=\delta} \operatorname{lm}(Q_i)G_i = \sum c_{jk}X^{\delta-\gamma^{jk}}S(G_j, G_k),$$

con $\exp(X^{\delta-\gamma^{jk}}S(G_j, G_k)) < \delta$. Los restos de la división de $S(G_j, G_k)$ por $G_1, \ldots, G_t$ son cero, entonces resulta:

$$S(G_j, G_k) = \sum Q_{jki}G_i, \qquad \text{con } Q_{jki} \in K[X_1, \ldots, X_n],$$

y por el algoritmo de la división tenemos:

$$\exp(Q_{jki}G_i) \leq \exp(S(G_j, G_k)).$$

Encontramos pues una expresión del siguiente tipo:

$$F = \sum_i Q'_iG_i, \quad \text{con } \exp(Q'G_i) < \delta.$$

Repitiendo el proceso tantas veces como sea necesario, llegamos a una expresión

$$F = \sum_i Q_iG_i,$$

en donde $\exp(F) = \max\{\exp(Q_iG_i) \mid i = 1, \ldots, t\}$, y como consecuencia $\exp(F) = \exp(Q_iG_i)$ para algún índice i, esto es:

$$\exp(F) = \exp(Q_iG_i) = \exp(Q_i) + \exp(G_i) \in \{\exp(G_1), \ldots, \exp(G_t\} + \mathbb{N}^n.$$

y $\mathbb{G}$ es una base de Groebner. □

Vamos ahora a buscar un mecanismo que nos permita construir una base de Groebner de un ideal $\mathfrak{a}$.

Teorema. 13.7. (Algoritmo de Buchberger)
Sea $\mathfrak{a}$ un ideal no nulo de $K[X_1, \ldots, X_n]$ con un sistema de generadores $\{F_1, \ldots, F_t\}$. Es posible construir una base de Groebner de $\mathfrak{a}$ siguiendo los siguientes pasos:
(1) Se define $\mathbb{G}_0 = \{F_1, \ldots, F_t\}$.
(2) Se define $\mathbb{G}_{n+1} = \cup\{R(S(F, G); \mathbb{G}_n) \neq 0 \mid F, G \in \mathbb{G}_n\}$.

Entonces cuando $\mathbb{G}_i = \mathbb{G}_{i+1}$, tenemos que $\mathbb{G}_i$ es una base de Groebner de $\mathfrak{a}$.

DEMOSTRACIÓN. Dado $\mathbb{G}_0 = \{G_1, \ldots, G_t\}$, si $R(S(F,G);\mathbb{G}_0) = 0$ para cada par $F, G \in \mathbb{G}_0$, entonces tenemos una base de Groebner. Si no lo es, existen $F, G \in \mathbb{G}_0$ tales que $R(S(F,G);\mathbb{G}_0) \neq 0$. Llamamos $G_{t+1} = R(S(F,G);\mathbb{G})$. Tenemos que $\mathcal{N}(G_{t+1}) \subseteq \overline{\Delta}$. Entonces, si definimos:

$$\mathbb{G}_{(1)} = \{G_1, \ldots, G_t, G_{t+1}\},$$

obtenemos una partición

$$\Delta^1, \ldots, \Delta^t, \Delta^{t+1}, \overline{\Delta^{(1)}},$$

siendo $\Delta^{t+1} \cup \overline{\Delta^{(1)}} = \overline{\Delta}$. Si $R(F;\mathbb{G}_0) = 0$, para $F \in K[X_1, \ldots, X_n]$, entonces $R(F;\mathbb{G}_{(1)}) = 0$. Y en el caso en que $R(S(G_i,G_j),\mathbb{G}_0) = 0$, también se tiene $R(S(G_i,G_j),\mathbb{G}_{(1)}) = 0$, por lo tanto el trabajo hecho lo podemos aprovechar.

Si para todo F, $G \in \mathbb{G}_{(1)}$ se verifica $R(S(F,G);\mathbb{G}_{(1)}) = 0$, entonces tenemos una base de Groebner. En el caso contrario tenemos un nuevo $G_{t+2} = R(S(F,G);\mathbb{G}_{(1)}) \neq 0$, y definimos un nuevo sistema de generadores $\mathbb{G}_{(2)} = \{G_1, \ldots, G_{t+1}, G_{t+2}\}$, teniendo que $\mathcal{N}(G_{t+2}) \subseteq \overline{\Delta^{(1)}}$.

Si en algún momento encontramos una base de Groebner, ya hemos terminado, en caso contrario tendríamos una cadena ascendente de sistemas de generadores:

$$\mathbb{G}_0 \subset \mathbb{G}_{(1)} \subset \cdots$$

Asociada tenemos una cadena ascendente de monoideales:

$$\exp(\mathbb{G}_0) + \mathbb{N}^n \subset \exp(\mathbb{G}_{(1)}) + \mathbb{N}^n \subset \cdots$$

Como consecuencia del Lema de Dickson esta cadena se estabiliza y por tanto existe un índice n tal que

$$\exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \exp(\mathbb{G}_{(n+1)}) + \mathbb{N}^n,$$

tenemos entonces

$$\exp(G_{t+n+1}) \in \exp(\mathbb{G}_{(n)}) + \mathbb{N}^n = \mathbb{N}^n \setminus \overline{\Delta^{(n)}},$$

pero $\exp(G_{t+n+1}) \in \overline{\Delta^{(n)}}$, lo que es una contradicción. □

En el proceso anterior obtenemos un sistema de generadores que es una base de Groebner, y que tiene, posiblemente, demasiados elementos. Veamos como optimizar el proceso de obtención de una base de Groebner.

Lema. 13.8.
Sea $\mathfrak{a}$ un ideal no nulo de $K[X_1, \ldots, X_n]$ y $\mathbb{G} = \{G_1, \ldots, G_t\}$ una base de Groebner de $\mathfrak{a}$. Sea $F \in \mathbb{G}$ un polinomio que verifica:

$$\exp(F) \in \{\exp(G) \mid F \neq G \in \mathbb{G}\} + \mathbb{N}^n,$$

entonces $\mathbb{G} \setminus \{F\}$ es una base de Groebner de $\mathfrak{a}$.

Una base de Groebner $\mathbb{G}$ de un ideal no nulo $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ se llama **minimal** si verifica:

(I) $\operatorname{lc}(F) = 1$ para cada $F \in \mathbb{G}$;
(II) $\exp(F) \notin \{\exp(G) \mid F \neq G \in \mathbb{G}\} + \mathbb{N}^n$ para cada $F \in \mathbb{G}$.

Simplemente eliminando los elementos que sobran tenemos la siguiente Proposición.

Proposición. 13.9.
Todo ideal no nulo $\mathfrak{a}$ de $K[X_1, \ldots, X_n]$ tiene una base de Groebner minimal.

Corolario. 13.10.
Dado un subconjunto $\mathbb{G} = \{G_1, \ldots, G_t\} \subseteq \mathfrak{a}$ de un ideal de $K[X_1, \ldots, X_n]$ son equivalentes:
(a) $\mathbb{G}$ es una base de Groebner minimal.
(b) $\{\exp(G_1), \ldots, \exp(G_t)\}$ es un sistema mínimo de generadores de $\operatorname{Exp}(\mathfrak{a})$.

Como consecuencia los términos líderes de una base de Groebner minimal están determinados de forma única y cada dos bases de Groebner minimales tienen el mismo número de elementos.

DEMOSTRACIÓN. La equivalencia (a) $\Leftrightarrow$ (b) es consecuencia directa de la definición.
El resto es consecuencia del Lema (10.5.) que asegura que cada monoideal tiene un único sistema de generadores minimal. □

Un ideal puede tener bases de Groebner minimales distintas. Para buscar la unicidad vamos a introducir las bases de Groebner reducidas. Una base de Groebner $\mathbb{G}$ de un ideal no nulo $\mathfrak{a}$ se llama **reducida** si verifica:

(I) $\operatorname{lc}(F) = 1$ para cada $F \in \mathbb{G}$;
(II) $\mathcal{N}(F) \cap (\{\exp(G) \mid F \neq G \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing$ para cada $F \in \mathbb{G}$.

Es claro que toda base de Groebner reducida de un ideal no nulo $\mathfrak{a}$ es una base de Groebner minimal.

Teorema. 13.11.
Cada ideal no nulo tiene una única base de Groebner reducida.

DEMOSTRACIÓN. Si $\mathbb{G}$ es una base de Groebner minimal, un elemento $F \in \mathbb{G}$ se llama **reducido** si

$$\mathcal{N}(F) \cap (\{\exp(G) \mid F \neq G \in \mathbb{G}\} + \mathbb{N}^n) = \varnothing.$$

Si $F \in \mathbb{G}$ es reducido, entonces es reducido en cualquier base de Groebner minimal $\mathbb{G}'$ que lo contenga y que verifique:

$$\{\exp(G) \mid G \in \mathbb{G}\} = \{\exp(G) \mid G \in \mathbb{G}'\}.$$

Definimos para cada $F \in \mathbb{G}$ los siguientes elementos:

$$\begin{array}{l} F' = R(F, \mathbb{G} \setminus \{F\}); \\ \mathbb{G}' = (\mathbb{G} \setminus \{F\}) \cup \{F'\}. \end{array}$$

$\mathbb{G}'$ es también una base de Groebner de $\mathfrak{a}$. Si $\exp(F) \neq \exp(F')$, entonces de las relaciones:

$$\begin{array}{l} F = \sum Q_G G + R(F; \mathbb{G} \setminus \{F\}) = \sum Q_G G + F' \\ \exp(F) = \max\{\{\exp(Q_G G) \mid G \in \mathbb{G} \setminus \{F\}\} \cup \{\exp(F')\}\}, \end{array}$$

y por ser todos los exponentes distintos, se tiene que existe $G \in \mathbb{G} \setminus \{F\}$ tal que $\exp(F) = \exp(Q_G G)$, lo que es una contradicción con el hecho de ser $\mathbb{G}$ una base de Groebner minimal. Tenemos entonces que $\mathbb{G}'$ es una base de Groebner y que F' es reducido. Aplicando este proceso a cada uno de los elementos obtenemos una base de Groebner reducida.

Para ver la unicidad, si $\mathbb{G}$ y $\mathbb{G}'$ son dos bases de Groebner reducidas, se verifica:

$$\operatorname{Exp}(\mathfrak{a}) = \exp(\mathbb{G}) + \mathbb{N}^n = \exp(\mathbb{G}') + \mathbb{N}^n.$$

Dado $F \in \mathbb{G}$ tenemos las relaciones siguientes:

$$\begin{array}{lll} \exp(F) = \exp(G') + \gamma, & G' \in \mathbb{G}', & \gamma \in \mathbb{N}^n; \\ \exp(G') = \exp(G) + \gamma', & G \in \mathbb{G}, & \gamma' \in \mathbb{N}^n; \end{array}$$

de donde se deduce que $\exp(F) = \exp(G) + \gamma + \gamma'$, y por ser $\mathbb{G}$ minimal tenemos $\gamma = 0 = \gamma'$. Entonces $\exp(F) = \exp(G')$ y como consecuencia tenemos la igualdad:

$$\exp(\mathbb{G}) = \exp(\mathbb{G}').$$

Dado ahora $F \in \mathbb{G}$, existe $G' \in \mathbb{G}'$ tal que $\exp(F) = \exp(G')$. Entonces $F - G'$ tiene todos sus términos menores que $\exp(F)$. Como $F - G' \in \mathfrak{a}$ tenemos $R(F - G'; \mathbb{G}) = 0$. Como $\mathbb{G}$ y $\mathbb{G}'$ son reducidas y $\exp(\mathbb{G}) = \exp(\mathbb{G}')$, tenemos

$$\mathcal{N}(F - G') \subseteq \overline{\Delta} = \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a}),$$

Para probar esta inclusión consideramos el siguiente desarrollo:

$$\begin{array}{l} \mathcal{N}(F - G') \cap (\exp(\mathbb{G}) + \mathbb{N}^n) = \\ \mathcal{N}(F - G') \cap (\cup\{\exp(L) + \mathbb{N}^n \mid L \in \mathbb{G}\}) = \\ \cup\{\mathcal{N}(F - G') \cap (\exp(L) + \mathbb{N}^n) \mid L \in \mathbb{G}\} = \\ \cup\{\mathcal{N}(F - G') \cap (\exp(L) + \mathbb{N}^n) \mid F \neq L \in \mathbb{G}\} = \\ \mathcal{N}(F - G') \cap (\{\exp(L) \mid F \neq L \in \mathbb{G}\} + \mathbb{N}^n) \subseteq \\ (\mathcal{N}(F) \cap (\{\exp(L) \mid F \neq L \in \mathbb{G}\} + \mathbb{N}^n)) \cup \\ \mathcal{N}(G') \cap (\{\exp(L) \mid G' \neq L \in \mathbb{G}'\} + \mathbb{N}^n)) = \varnothing \end{array}$$

Entonces $R(F - G'; \mathbb{G}) = F - G'$, de donde $F = G'$. □

14. Aplicaciones de las Bases de Groebner

Vamos a estudiar aplicaciones de la teoría de bases de Groebner hasta ahora desarrollada. En primer lugar estudiamos las aplicaciones clásicas de las bases de Groebner en orden a calcular con elementos en el anillo $K[X_1,\ldots,X_n]$. La última parte la dedicamos al cálculo de la dimensión en algunos ejemplos de anillos cocientes de anillos de polinomios.

Problema de pertenencia

Problema. 14.1.
Sea $\mathfrak{a}$ un ideal izquierda de $K[X_1,\ldots,X_n]$ con un sistema de generadores $\{F_1,\ldots,F_r\}$; dado $F \in K[X_1,\ldots,X_n]$, nos planteamos el problema de determinar si $F \in \mathfrak{a}$.

Esto se hace como sigue: se calcula una base de Groebner $\mathbb{G} = \{G_1,\ldots,G_t\}$ de $\mathfrak{a}$; entonces tenemos $F \in \mathfrak{a}$ si, y sólo si, $R(F;\mathbb{G}) = 0$.
Es posible también obtener una expresión de F como combinación lineal de los generadores originales F_1, …, F_r. Para ello únicamente hay que tener en cuenta que, por el algoritmo de la división, tenemos una expresión de la forma:

$$F = Q_1G_1 + \cdots + Q_tG_t,$$

y como los G_i se obtienen haciendo s–polinomios a partir de los F_j, tenemos que es posible dar la expresión deseada.

Igualdad de ideales

Problema. 14.2.
Sean $\mathfrak{a}_1$ y $\mathfrak{a}_2$ ideales de $K[X_1,\ldots,X_n]$ con sistemas de generadores $\{F_1^1,\ldots,F_{r_1}^1\}$ y $\{F_1^2,\ldots,F_{r_2}^2\}$, respectivamente. El problema es determinar cuando $\mathfrak{a}_1 = \mathfrak{a}_2$.

Conseguimos bases de Groebner reducidas $\mathbb{G}_1$ y $\mathbb{G}_2$ de $\mathfrak{a}_1$ y $\mathfrak{a}_2$, respectivamente. Por la unicidad de las bases de Groebner reducidas, tenemos $\mathfrak{a}_1 = \mathfrak{a}_2$ si, y sólo si, $\mathbb{G}_1 = \mathbb{G}_2$.

Representantes canónicos

Problema. 14.3.
Dado un ideal $\mathfrak{a}$ de $K[X_1,\ldots,X_n]$ el problema es dar un criterio, y un método, para determinar un representante canónico en cada clase del cociente $K[X_1,\ldots,X_n]/\mathfrak{a}$.

En primer lugar, dado $\mathfrak{a}$, construimos una base de Groebner $\mathbb{G}$ de $\mathfrak{a}$. Para cada $F \in K[X_1,\ldots,X_n]$ consideramos el resto $R(F;\mathbb{G})$ y es claro que se verifica:

$$F+\mathfrak{a} = R(F;\mathbb{G})+\mathfrak{a}.$$

Además, $R(F,\mathbb{G})$ es único verificando la igualdad anterior y $\mathcal{N}(R(F;\mathbb{G})) \subseteq \overline{\Delta} = \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a})$, ver Proposición (13.3.). Este elemento $R(F;\mathbb{G})$ lo llamamos la forma normal de la clase de F con respecto a $\mathbb{G}$.
El comportamiento de la forma normal es bueno respecto a combinaciones K–lineales, ya que si a_1, $a_2 \in \mathbb{C}$ y $F_1, F_2 \in K[X_1,\ldots,X_n]$, entonces se verifica: $R(a_1F_1+a_2F_2;\mathbb{G}) = a_1R(F_1;\mathbb{G})+a_2R(F_2;\mathbb{G})$.
Es claro que por el algoritmo de la división tenemos:

$$F_i = Q_1^iG_1+\cdots+Q_t^iG_t+R(F_i;\mathbb{G}),$$

entonces se verifica:

$$\begin{gathered}a_1F_1+a_2F_2 = \\ a_1Q_1^1G_1+\cdots+a_1Q_t^1G_t+a_1R(F_1;\mathbb{G})+a_2Q_1^2G_1+\cdots+a_2Q_t^2G_t+a_2R(F_2;\mathbb{G}) = \\ (a_1Q_1^1+a_2Q_1^2)G_1+\cdots+(a_1Q_t^1+a_2Q_t^2)G_t+a_1R(F_1;\mathbb{G})+a_2R(F_2;\mathbb{G}),\end{gathered}$$

de donde tenemos el resultado, ya que

$$\mathcal{N}(a_1R(F_1;\mathbb{G})+a_2R(F_2;\mathbb{G})) \subseteq \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a}),$$

y por tanto $R(a_1F_1+a_2F_2;\mathbb{G}) = a_1R(F_1;\mathbb{G})+a_2R(F_2;\mathbb{G})$. Tenemos entonces, para cualesquiera F_1, $F_2 \in K[X_1,\ldots,X_n]$, las equivalencias entre los siguientes enunciados:

$$\begin{aligned}&F_1+\mathfrak{a} = F_2+\mathfrak{a}.\\ &F_1-F_2 \in \mathfrak{a}.\\ &R(F_1-F_2;\mathbb{G}) = 0.\\ &R(F_1;\mathbb{G}) = R(F_2;\mathbb{G}).\end{aligned}$$

Como consecuencia, cada elemento de $K[X_1,\ldots,X_n]/\mathfrak{a}$ está unívocamente determinado, y determina, un elemento R de $K[X_1,\ldots,X_n]$ con $\mathcal{N}(R) \subseteq \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a})$. Para estos elementos las operaciones en $K[X_1,\ldots,X_n]/\mathfrak{a}$ están definidas exactamente por estos representantes por la regla:

$$a_1(R_1+\mathfrak{a})+a_2(R_2+\mathfrak{a}) = (a_1R_1+a_2R_2)+\mathfrak{a}.$$

Ideales cofinitos

Pasamos ahora a estudiar el caso de ideales cofinitos, esto es, ideales $\mathfrak{a}$ de $K[X_1,\ldots,X_n]$ tales que el cociente $K[X_1,\ldots,X_n]/\mathfrak{a}$ es de dimensión finita como K–espacio vectorial.

K–base del cociente

Problema. 14.4.
Se trata de dar un método que permita calcular una base del cociente $K[X_1,\ldots,X_n]/\mathfrak{a}$.

Para cada clase $F+\mathfrak{a}$ de $K[X_1,\ldots,X_n]/\mathfrak{a}$, considerando una base de Groebner de $\mathfrak{a}$, tenemos un representante R de la clase $F+\mathfrak{a}$ tal que $\mathcal{N}(R)\subseteq\mathbb{N}^n\setminus\operatorname{Exp}(\mathfrak{a})$. De aquí resulta que R se puede escribir en la forma

$$R=\sum_\alpha c_\alpha X^\alpha,$$

con $\alpha\notin\{\exp(G):\ G\in\mathbb{G}\}+\mathbb{N}^n=\operatorname{Exp}(\mathfrak{a})$ y $c_\alpha\in K$. Tenemos entonces que $\{X^\beta\mid\ \beta\in\mathbb{N}^n\setminus\operatorname{Exp}(\mathfrak{a})\}$ es un sistema de generadores linealmente independiente de $K[X_1,\ldots,X_n]/\mathfrak{a}$; esto resuelve el problema.

Como subproducto podemos determinar cuándo un ideal a la izquierda es cofinito; lo es si, y sólo si, el cardinal del conjunto $\mathbb{N}^n\setminus\operatorname{Exp}(\mathfrak{a})$ es finito. Este resultado lo mejoraremos más adelante al estudiar la dimensión de los cocientes $K[X_1,\ldots,X_n]/\mathfrak{a}$.

Operaciones en el cociente

Problema. 14.5.
Dar un criterio que permita calcular las operaciones en el cociente $K[X_1,\ldots,X_n]/\mathfrak{a}$ cuando $\mathfrak{a}$ es un ideal (cofinito) de $K[X_1,\ldots,X_n]$.

Supuesto que $\mathfrak{a}$ es un ideal cofinito, las clases del cociente $S=K[X_1,\ldots,X_n]/\mathfrak{a}$ tienen una K–base finita, y como S es un anillo, tenemos un producto interno en S. Pero S es una K–álgebra finito–dimensional, luego este producto se puede describir completamente en términos de los productos de los elementos de una K–base. El cálculo se realiza considerando una base de Groebner $\mathbb{G}$ y calculando los restos de la división por $\mathbb{G}$.

Caracterización de ideales cofinitos

Ya conocemos que un ideal a la izquierda $\mathfrak{a}$ de $K[X_1,\ldots,X_n]$ es cofinito si, y sólo si, $\mathbb{N}^n\setminus\operatorname{Exp}(\mathfrak{a})$ es finito. Vamos a buscar una caracterización más sencilla.

Proposición. 14.6.
Sea $\mathfrak{a}$ un ideal a la izquierda de $K[X_1, \ldots, X_n]$ con base de Groebner reducida $\mathbb{G}$. Son equivalentes los siguientes enunciados:

(a) $\mathfrak{a}$ es cofinito.
(b) Para cada indeterminada X_i existen $G_j \in \mathbb{G}$ y $\nu_i \in \mathbb{N}$ tales que $\operatorname{lm}(G_j) = X_i^{\nu_i}$.

DEMOSTRACIÓN. (a)⇒(b). Como $\mathfrak{a}$ es cofinito, dado X_i existe $\nu_i \in \mathbb{N}$ tal que $X_i^{\nu_i}$ es el término líder de un polinomio en $\mathfrak{a}$, entonces $(0, \ldots, \nu_i, \ldots, 0) \in \operatorname{Exp}(\mathfrak{a}) = \exp(\mathbb{G}) + \mathbb{N}^n$. Llamemos $\alpha^j = \exp(G_j)$ para cada $G_j \in \mathbb{G}$. Existen $j \in \{1, \ldots, t\}$ y $\gamma \in \mathbb{N}^n$ tales que

$$(0, \ldots, \nu_i, \ldots, 0) = \alpha^j + \gamma,$$

entonces $\alpha_h^j = 0 = \gamma_h$ si $h \neq i$. Luego $\exp(G_j) = (0, \ldots, \mu_i, \ldots, 0)$ para algún $\mu_i \in \mathbb{N}$, esto es, $\operatorname{lm}(G_j) = X_i^m$ para algún $m \in \mathbb{N}$.
(b)⇒(a). Consideramos $\alpha \in \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a})$. Por hipótesis, para cada X_i existe G_j tal que $\operatorname{lt}(G_j) = X_i^{\nu_i}$. Si $\alpha_i \geq \nu_i$, entonces tenemos una expresión del siguiente tipo:

$$\alpha = (0, \ldots, \nu_i, \ldots, 0) + (\alpha_1, \ldots, \alpha_i - \nu_i, \ldots, \alpha_n) \in \exp(G_j) + \mathbb{N}^n \subseteq \operatorname{Exp}(\mathfrak{a}),$$

lo que es una contradicción, y por tanto necesariamente $\alpha_i < \nu_i$, para cada índice i. En consecuencia existe un número finito de elementos $\alpha \in \mathbb{N}^n \setminus \operatorname{Exp}(\mathfrak{a})$ y por tanto $\mathfrak{a}$ es cofinito. □

15. Aplicaciones de las Bases de Groebner, II

Eliminación de variables

Dado un sistema de ecuaciones polinómicas: $F_i = 0\}_{i=1,\dots,s}$, siendo cada $F_i \in K[X_1,\dots,X_n]$, una solución al sistema es un elemento $(a_1,\dots,a_n) \in K^n$ tal que $F_i(a_1,\dots,a_n) = 0$ para cada índice i.

Observar que si llamamos $\mathfrak{a}$ al ideal generado por $\{F_1,\dots,F_s\}$, entonces para cada sistema de generadores $\{G_1,\dots,G_t\}$ de $\mathfrak{a}$ un elemento $(a_1,\dots,a_n)$ es una solución del sistema $F_i = 0\}_{i=1,\dots,s}$ si y sólo si es una solución del sistema $G_j = 0\}_{j=1,\dots,t}$.

Esto significa que los sistemas que tenemos que resolver son aquellos para los que $\{F_1,\dots,F_s\}$ es una base de Groebner, si es necesario reducida, de un cierto ideal.

En el caso en que los F_i son polinomios lineales el sistema $F_i = 0\}_{i=1,\dots,s}$ se resuelve por el método de Gauss–Jordan. En ese caso se van eliminando variables: X_1, X_2, etc., hasta llegar a ecuaciones en las que cada variable “libre"se expresa en función de unas variables “dependientes".

Ejemplo. 15.1.
Consideramos el sistema de ecuaciones lineales

$$\left.\begin{array}{r} X_1 + X_2 - X_3 + 2X_4 - 1 = 0 \\ 2X_1 + X_2 + X_3 - X_4 + 2 = 0 \\ X_1 - X_2 + 5X_3 - 8X_4 + 7 = 0 \end{array}\right\}$$

Su solución es la solución del sistema:

$$\left.\begin{array}{rrrrr} X_1 & & +2X_3 & -3X_4 & +3 = 0 \\ & X_2 & -3X_3 & +5X_4 & -4 = 0 \end{array}\right\}$$

Observa que si consideramos el orden lexicográfico con $X_1 > X_2 > X_3 > X_4$, y llamamos $\mathfrak{a}$ al ideal $(X_1 + X_2 - X_3 + 2X_4 - 1, 2X_1 + X_2 + X_3 - X_4 + 2, X_1 - X_2 + 5X_3 - 8X_4 + 7)$, una base de Groebner es: $\{X_1 + 2X_3 - 3X_4 + 3, X_2 - 3X_3 + 5X_4 - 4\}$. Además una base de Groebner de $\mathfrak{a}_1 := \mathfrak{a} \cap K[X_2,X_3,X_4]$ es $\mathbb{G}_1 = \{X_2 - 3X_3 + 5X_4 - 4\}$.

Este proceso podemos repetirlo si consideramos un sistema de ecuaciones polinómicas no lineales $F_i = 0\}_{i=1,\dots,s}$. Si $\{F_i \mid i = 1,\dots,s\}$ es una base de Groebner del ideal correspondiente, al que llamaremos $\mathfrak{a}$, definimos el ***i*–ésimo ideal de eliminación**, con respecto al orden lexicográfico con $X_1 > \cdots > X_n$, como $\mathfrak{a}_i := \mathfrak{a} \cap K[X_{i+1},\dots,X_n]$.

Teorema. 15.2.
Sea $\mathbb{G} = \{G_1,\dots,G_t\}$ una base de Groebner de un ideal no nulo $\mathfrak{a} \subseteq K[X_1,\dots,X_n]$ con respecto al orden lexicográfico con $X_1 > \cdots > X_n$. Entonces $\mathbb{G} \cap K[X_{i+1},\dots,X_n]$ es una base de Groebner del i–ésimo ideal de eliminación $\mathfrak{a}_i = \mathfrak{a} \cap K[X_{i+1},\dots,X_n]$.

DEMOSTRACIÓN. Supongamos que $\mathbb{G}_i = \{G_k, \ldots, G_t\}$. Dado $F \in \mathfrak{a}_i$ se tiene $\exp(F) \in \Delta^j$ para algún $j = k, \ldots, t$, ya que F no tiene monomios en los que aparezcan $X_1, \ldots, X_i$. Por lo tanto $\exp(F) \in \{\exp(G_k), \ldots, \exp(G_t)\} + \mathbb{N}^n$, y se tiene $\operatorname{Exp}(\mathfrak{a}_i) = \{\exp(G_k), \ldots, \exp(G_t)\} + \mathbb{N}^n$. □

La aplicación de este resultado es como sigue: Dado un sistema de ecuaciones $F_j = 0\}_{j=1,\ldots,s}$ en el que $\mathbb{G} := \{F_j \mid j = 1, \ldots, s\}$ es una base de Groebner, ordenamos los elementos de $\mathbb{G}$ de forma que $\mathbb{G}_i = \{F_{k_i}, F_{k_i+1}, \ldots, F_s\}$ con $1 \leq k_i \leq k_{i+i} \leq s$, para cada índice $i = 0, 1, \ldots, n-1$. Entonces comenzamos resolviendo el sistema $F_j = 0\}_{j=k_{n-1},\ldots,s}$. A continuación, con los valores obtenidos resolvemos el sistema $F_j = 0\}_{j=k_{n-2},\ldots,s}$, y así proseguimos hasta resolver el sistema inicial $F_j = 0\}_{j=1,\ldots,t}$.

Ejercicio. 15.3.
Resuelve en $\mathbb{C}$ el sistema

$$\left.\begin{aligned} X^3 - 2XY + Y^3 = 0 \\ X^5 - 2X^2Y^2 + Y^5 = 0 \end{aligned}\right\}$$

Calculamos una base de Groebner para el ideal $\mathfrak{a} = (X^3 - 2XY + Y^3, X^5 - 2X^2Y^2 + Y^5)$, con respecto al orden lexicográfico con $X > Y$. Éste es:

$$\{X^3 - 2XY + Y^3, 200XY^2 + 193Y^9 + 158Y^8 - 45Y^7 - 456Y^6 + 50Y^5 - 100Y^4, \\ Y^{10} - Y^8 + 2Y^7 + 2Y^6\}.$$

Al resolver $Y^{10} - Y^8 + 2Y^7 + 2Y^6 = Y^6(Y-1)^2(Y^2 + 2Y + 2) = 0$ tenemos las raíces

$$y_1 = 0, \quad y_2 = 1, \quad y_3 = -1 + i, \quad y_4 = -1 - i.$$

Para cada uno de estos valores: y_1, y_2 e y_3, tenemos que resolver las ecuaciones

$$\left.\begin{aligned} X^3 - 2XY + Y^3 = 0 \\ 200XY^2 + 193Y^9 + 158Y^8 - 45Y^7 - 456Y^6 + 50Y^5 - 100Y^4 = 0 \end{aligned}\right\}$$

$y_1 = 0$. El sistema es:

$$\left.\begin{aligned} X^3 = 0 \\ 0 = 0 \end{aligned}\right\}$$

La única solución es: $(0, 0)$.
$y_2 = 1$. El sistema es:

$$\left.\begin{aligned} X^3 - 2X + 1 = 0 \\ 200X - 200 = 0 \end{aligned}\right\}$$

La única solución es: $(1, 1)$.
$y_3 = -1 \pm i$. El sistema es:

$$\left.\begin{aligned} X^3 - 2(-1 \pm i)X + (-1 \mp i) = 0 \\ -400i(X + 1 \mp i) = 0 \end{aligned}\right\}$$

La única solución es: $(-1 \mp i, -1 \pm i)$.
Por lo tanto el sistema tiene cuatro soluciones: $(0, 0)$, $(1, 1)$, $(-1 - i, -1 + i)$ y $(-1 + i, -1 - i)$.

Intersección de ideales

Dados dos ideales $\mathfrak{a}$ y $\mathfrak{b}$ del anillo $K[X_1,\ldots,X_n]$, se trata de determinar la intersección $\mathfrak{a}\cap\mathfrak{b}$.

Vamos a hacer uso de la técnica de eliminación de variables, para esto introducimos una nueva variable T, y consideramos la extensión de anillos

$$\omega : K[X_1,\ldots,X_n] \longrightarrow K[T,X_1,\ldots,X_n].$$

El ideal $\mathfrak{a}$ se extiende al ideal $\mathfrak{a}^e$ en $K[T,X_1,\ldots,X_n]$ generado por los mismos elementos, esto es, si $\mathfrak{a} = \langle F_1,\ldots,F_s\rangle$, entonces $\mathfrak{a}^e = K[T,X_1,\ldots,X_n]\mathfrak{a} = \langle F_1,\ldots,F_s\rangle$ en $K[T,X_1,\ldots,X_n]$. De forma análoga tenemos para $\mathfrak{b} = \langle G_1,\ldots,G_t\rangle$.

Teorema. 15.4.
Sean $\mathfrak{a} = \langle F_1,\ldots,F_s\rangle$ y $\mathfrak{b} = \langle G_1,\ldots,G_t\rangle$, ideales de $K[X_1,\ldots,X_n]$. Se considera una nueva variable T, la extensión $\omega : K[X_1,\ldots,X_n] \longrightarrow K[T,X_1,\ldots,X_n]$ y el ideal $\mathfrak{c} := T\mathfrak{a}^e + (1-T)\mathfrak{b}^e \subseteq K[T,X_1,\ldots,X_n]$. Se verifica

$$\mathfrak{a}\cap\mathfrak{b} = \mathfrak{c}\cap K[X_1,\ldots,X_n],$$

esto es, $\mathfrak{a}\cap\mathfrak{b}$ es el primer ideal eliminación de $\mathfrak{c}$ con respecto al orden lexicográfico con $T > X_1 > \cdots > X_n$.

DEMOSTRACIÓN. Dado $F \in \mathfrak{a}\cap\mathfrak{b}$ se tiene $F = TF + (1-T)F$, luego $\mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{c}\cap K[X_1,\ldots,X_n]$. Sea ahora $F \in \mathfrak{c}\cap K[X_1,\ldots,X_n]$, existen U_i, $V_j \in K[T,X_1,\ldots,X_n]$ tales que

$$F = T\sum_{i=1}^{s} U_iF_i + (1-T)\sum_{j=1}^{t} V_jG_j.$$

Al evaluar esta expresión en $T = 1$ se obtiene

$$F = \sum_{i=1}^{s} U_i(1,X_1,\ldots,X_n)F_i(X_1,\ldots,X_n) \in \mathfrak{a},$$

y al evaluar en $T = 0$ se tiene

$$F = \sum_{j=1}^{t} V_j(0,X_1,\ldots,X_n)G_j(X_1,\ldots,X_n) \in \mathfrak{b}.$$

Luego $F \in \mathfrak{a}\cap\mathfrak{b}$. □

Ejercicio. 15.5.
Determina la intersección de los ideales $\mathfrak{a} = (X,Y)$ *y* $\mathfrak{b} = (X-1, Y-1)$ *en* $K[X,Y]$.

SOLUCIÓN. Introducimos una nueva variable T. Un sistema de generadores para $T\mathfrak{a} + (1-T)\mathfrak{b}$ es $\{TX, TY, (1-T)(X-1), (1-T)(Y-1)\}$. Una pequeña manipulación nos conduce al sistema de generadores: $\{TX, TY, T+X-1, X-Y\}$. A partir de aquí una base de Groebner es: $\{TX, TY, T+X-1, X-Y, Y^2-Y\}$, y una base de Groebner reducida es: $\{TX, TY, T+Y-1, X-Y, Y^2-Y\}$.
El primer ideal de eliminación tiene como base de Groebner $\{X-Y, Y^2-Y\}$. Por lo tanto $\mathfrak{a} \cap \mathfrak{b} = (X-Y, Y^2-Y)$. □

Cociente de ideales

Una aplicación de la intersección de ideales es el cociente de dos ideales. Dados $\mathfrak{a}$, $\mathfrak{b} \subseteq K[X_1,\ldots,X_n]$, recordar que el **cociente** de $\mathfrak{a}$ y $\mathfrak{b}$ se define como

$$(\mathfrak{a} : \mathfrak{b}) = \{F \in K[X_1,\ldots,X_n] \mid F\mathfrak{b} \subseteq \mathfrak{a}\}.$$

Observa que $(\mathfrak{a} : \mathfrak{b}) = \cap\{(\mathfrak{a} : G) \mid G \in \mathfrak{b}\}$, y si $\{G_j \mid j = 1,\ldots,t\}$ es un sistema de generadores de $\mathfrak{b}$, entonces

$$(\mathfrak{a} : \mathfrak{b}) = \cap\{(\mathfrak{a} : G_j) \mid j = 1,\ldots,t\}.$$

Para realizar el cálculo efectivo del cociente de dos ideales, basta pues determinar $(\mathfrak{a} : G)$.

Proposición. 15.6.
Dados $\mathfrak{a}$ *un ideal de* $K[X_1,\ldots,X_n]$ *y* $G \in K[X_1,\ldots,X_n]$ *se verifica:*

$$G(\mathfrak{a} : G) = \mathfrak{a} \cap (G).$$

Como consecuencia, se tiene: $(\mathfrak{a} : G) = \frac{1}{G}(\mathfrak{a} \cap (G))$.

DEMOSTRACIÓN. Sea $F \in G(\mathfrak{a} : G)$, entonces $F = GH$ para algún $H \in (\mathfrak{a} : G)$, entonces $F = GH \in \mathfrak{a} \cap G$. Por otro lado, si $F \in \mathfrak{a} \cap (G)$, entonces $F = GH$ para algún $H \in K[X_1,\ldots,X_n]$, y como $F \in \mathfrak{a}$, entonces $GH \in \mathfrak{a}$ y por tanto $H \in (\mathfrak{a} : G)$, esto es, $F \in G(\mathfrak{a} : G)$. □

Como el cálculo de la intersección de dos ideales de $K[X_1,\ldots,X_n]$ es posible realizarlo mediante métodos computacionales, resulta que también es posible realizar el cociente de dos ideales.

Ejercicio. 15.7.
Dados $\mathfrak{a} = (X^2 + XY - Y^2 + 1, XY^2 + X - 1)$ *y* $G = X - Y$, *determina* $(\mathfrak{a} : G)$.

SOLUCIÓN. Consideramos $\mathfrak{a} \cap (G)$. Una base de Groebner es: $\{XY^6 + XY^4 - XY^3 - XY^2 - XY - 2X - Y^7 - Y^5 + Y^4 + Y^3 + Y^2 + 2Y, X^2 - XY^4 + X + Y^5 - Y^2 - Y\}$; sin embargo tenemos que calcular $\frac{1}{G}(\mathfrak{a} \cap (G))$. Al dividir por G tenemos que una base de $(\mathfrak{a} : G)$ es: $\{Y^6 + Y^4 - Y^3 - Y^2 - Y - 2, X - Y^4 + Y + 1\}$. □

Cálculo del máximo común divisor de dos polinomios

Dados $F, G \in K[X_1, \ldots, X_n]$, como $K[X_1, \ldots, X_n]$ es un DFU, existen el m.c.d., D y el m.c.m., M, de F y G, y verifican $FG = DM$. Por tanto $D = \frac{FG}{M}$. Por la definición de m.c.m. se tiene $(M) = (F) \cap (G)$. Tenemos por tanto un método para determinar el m.c.d. de F y G; sólo tenemos que calcular $(F) \cap (G) = (TF, (1 - T)G) \cap K[X_1, \ldots, X_n]$; M será el único elemento de la base de Groebner de $(F) \cap (G)$. Para calcular D realizamos la división $\frac{FG}{M}$.

16. Ejercicios

Órdenes

Ejercicio. 16.1.
Prueba que un orden total en un conjunto X es un buen orden si, y solo si, cada cadena descendente es estacionaria.

SOLUCIÓN

Representación de polinomios

Ejercicio. 16.2.
Ordena los monomios

$$X^3Z^2, X^2Y^2Z, XZ^2, Y^2Z, X^3Y, X^3Z, X^2Y, Y^2Z^2.$$

(1) Para el orden lexicográfico dado por $X > Y > Z$.
(2) Para el orden lexicográfico graduado correspondiente y
(3) Para el orden lexicográfico graduado inverso correspondiente.

SOLUCIÓN

Ejercicio. 16.3.
Ordena los monomios

$$X^2Z, X^2Y^2Z, XY^2Z, X^3Y, X^3Z^2, X^2, X^2YZ^2, X^2Z^2.$$

(1) para el orden monomial lexicográfico dado por $X > Y > Z$.
(2) Para el orden lexicográfico graduado correspondiente.
(3) Para el orden lexicográfico graduado inverso correspondiente.

SOLUCIÓN

Ejercicio. 16.4.
Estudia los siguientes enunciados:

(1) Escribe explícitamente los diez primeros monomios del anillo $K[X,Y]$ para el orden lex *y para el orden* invgrlex *dados por $X > Y$.*

(2) Escribe explícitamente todos los monomios de $K[X,Y,Z]$ de grado total menor o igual a 2 en orden lexicográfico y en orden lexicográfico graduado.

SOLUCIÓN

Ejercicio. 16.5.
Razona que existen $n!$ ordenaciones monomiales lexicográficas distintas sobre $K[X_1,\dots,X_n]$. Y razona que existen $n!$ ordenaciones grlex *distintas y $n!$ ordenaciones* invgrlex *distintas sobre $K[X_1,\dots,X_n]$.*

SOLUCIÓN

Algoritmo de la división

Ejercicio. 16.6.
Usando el orden invgrlex *para $X > Y$:*

(1) Halla el resto de $X^7Y^2 + XY^2 + Y^2$ módulo $\{XY^2 - X, X - Y^3\}$.

(2) Halla el resto de $X^7Y^2 + XY^2 + Y^2$ módulo $\{X - Y^3, XY^2 - X\}$.

SOLUCIÓN

Ejercicio. 16.7.
Usando el orden invgrlex *para $X > Y$:*

(1) Halla el resto de $X^2Y + XY^2 + Y^2$ módulo $\{Y^2 - 1, XY - 1\}$.
(2) Halla el resto de $X^2Y + XY^2 + Y^2$ módulo $\{XY - 1, Y^2 - 1\}$.

SOLUCIÓN

Ejercicio. 16.8.
Haz la división de $F = X^3Y^3 + 3X^2Y^4$ por $G = XY^4$ en $K[X,Y]$ cuando consideramos el orden lexicográfico (con la ordenación de indeterminadas $X > Y$).

SOLUCIÓN

Ejercicio. 16.9.
Haz la división de $F = X^2+X-Y^2+Y$ *por* $\{G_1 = XY+1, G_2 = X+Y\}$ *en* $K[X,Y]$ *cuando consideramos el orden lexicográfico (con la ordenación de indeterminadas* $X > Y$*).*

SOLUCIÓN

Ejercicio. 16.10.
Haz la división de $F = X^2+X-Y^2+Y$ *por* $\{G_1 = X+Y, G_2 = XY+1\}$ *en* $K[X,Y]$ *cuando consideramos el orden lexicográfico (con la ordenación de indeterminadas* $X > Y$*).*

SOLUCIÓN

Ejercicio. 16.11.
Dados los polinomios

$$\begin{aligned} F &= X^3Y^2Z + X^2Y^3Z^2 + 2XYZ - Y^4 + 1; \\ G_1 &= XY^2 + YZ + Y + 2Z; \\ G_2 &= XZ^2 + Y - Z + 1; \\ G_3 &= XYZ + Y^2Z^2 + X - Y + 2. \end{aligned}$$

(1) Determina la división de F *por* $\{G_1, G_2, G_3\}$ *con el orden lexicográfico para la ordenación dada por* $X > Y > Z$.
(2) Haz lo mismo con el orden graduado lexicográfico.
(3) Haz lo mismo con el orden graduado lexicográfico inverso.

SOLUCIÓN

Ejercicio. 16.12.
Dados los polinomios

$$\begin{aligned} H &= X^2Y^2 - X^2Z - XY^2Z^3 + XY^2Z + XYZ + 3XY - XZ^2 + Y^3Z^2 - Y^2 - YZ - Z - 1 \\ G_1 &= XY^2 + YZ + Y + 2Z; \\ G_2 &= XZ^2 + Y - Z + 1; \\ G_3 &= XYZ + Y^2Z^2 + X - Y + 2. \end{aligned}$$

(1) Determina la división de H *por* $\{G_1, G_2, G_3\}$ *con el orden lexicográfico para la ordenación dada por* $X > Y > Z$.
(2) Haz lo mismo con el orden graduado lexicográfico.
(3) Haz lo mismo con el orden graduado lexicográfico inverso.

SOLUCIÓN

Ejercicio. 16.13.
Dados los polinomios

$$\begin{aligned}
&F = X^3Y^2Z + X^2Y^3Z^2 + 2XYZ - Y^4 + 1;\\
&H = X^2Y^2 - X^2Z - XY^2Z^3 + XY^2Z + XYZ + 3XY - XZ^2 + Y^3Z^2 - Y^2 - YZ - Z - 1\\
&G_1 = XY^2 + YZ + Y + 2Z;\\
&G_2 = XZ^2 + Y - Z + 1;\\
&G_3 = XYZ + Y^2Z^2 + X - Y + 2;
\end{aligned}$$

Responde a las siguientes preguntas:

(1) ¿Pertenece F al ideal generado por $\{G_1, G_2, G_3\}$?
(2) ¿Pertenece H al ideal generado por $\{G_1, G_2, G_3\}$?

SOLUCIÓN

Ejercicio. 16.14.
Sea K un cuerpo y $X_1, \ldots, X_n$ indeterminadas sobre K. Dados dos polinomios F, G en el anillo $K[X_1, \ldots, X_n]$:

(1) Prueba que $FG = \text{m.c.d.}\{F, G\}\,\text{m.c.m.}\{F, G\}$.
(2) Prueba que $(F) \cap (G) = (\text{m.c.m.}\{F, G\})$.
(3) ¿Ocurre lo mismo con $(F) + (G)$ y $(\text{m.c.d.}\{F, G\})$?

SOLUCIÓN

Ejercicio. 16.15.
Divide, con el orden lexicográfico, el polinomio F por el conjunto, ordenado, de polinomios $\mathbb{H} = \{H_1, H_2\}$, siendo:

(1) $F = XYZ$; $H_1 = X + Z$; $H_2 = Y - Z$.
(2) $F = XY^2 - X$; $H_1 = XY + 1$; $H_2 = Y^2 - 1$.
(3) $F = XY^2 - X$; $H_1 = Y^2 - 1$; $H_2 = XY + 1$.

SOLUCIÓN

Ejercicio. 16.16.
Si K es un cuerpo el anillo $K[X]$ es un DE, y por tanto el $\operatorname{m.c.d.}$ D de dos elementos $F, G \in K[X]$ se escribe $D = FC_1 + GC_2$, la identidad de Bezout, con $C_1, C_2 \in K[X]$.
Por otro lado tenemos que $\mathbb{Q}[X, Y]$ no es un DE y no se verifica, en general, la identidad de Bezout.

(1) *Da un ejemplo de dos polinomios $F, G \in \mathbb{Q}[X, Y]$ cuyo $\operatorname{m.c.d.}$ no se pueda escribir como una combinación de F y G.*
(2) *Prueba que esto ocurre si, y solo si, $(F, G) \subseteq \mathbb{Q}[X, Y]$ no es un ideal principal.*

SOLUCIÓN

Ejercicio. 16.17.
Haz la división de F por $\{G_1, G_2, G_3\}$, siendo:$F = X^5Y^2 + X^5Z^2 + Y^3Z^3$,$G_1 = (X + Y + Z)^2 - 1$,$G_2 = XY + YZ^2 + XZ^3 + Y$,$G_3 = X^7Y - X^4Y^3Z + 4Y^5Z^2 - 2$,en los siguientes casos:

(1) *con el orden lexicográfico.*
(2) *con el orden lexicográfico graduado.*
(3) *con el orden lexicográfico graduado inverso.*

SOLUCIÓN

Ideales monomiales

Ejercicio. 16.18.
Sean $\mathfrak{a}, \mathfrak{b} \subseteq K[X_1, \dots, X_n]$ ideales monomiales generados por $\{A_1, \dots, A_s\}$ y $\{B_1, \dots, B_t\}$ respectivamente.

(1) *Demuestra que $\mathfrak{a} \cap \mathfrak{b}$ es un ideal monomial.*
(2) *Demuestra que $\{M_{i,j} \mid i = 1, \dots, s, j = 1, \dots, t\}$, $M_{i,j}$ es un m.c.m. de A_i y B_j, es un sistema de generadores de $\mathfrak{a} \cap \mathfrak{b}$.*
(3) *Calcula la intersección de los ideales $\mathfrak{a} = (X, Y^2Z, YZ^2)$ y $\mathfrak{b} = (X^3YZ, X^2Y, Y^2Z^3)$ en el anillo $K[X, Y, Z]$.*

SOLUCIÓN

SOLUCIÓN. Ejercicio (16.18.)
(1).Dado $F \in \mathfrak{a} \cap \mathfrak{b}$, si la descomposición en monomios de F es $F = M_1 + \cdots + M_r$, como $F = M_1 + \cdots + M_r \in \mathfrak{a}$ y $\mathfrak{a}$ es un ideal monomial, resulta $M_1, \dots, M_r \in \mathfrak{a}$, y de la misma forma $M_1, \dots, M_r \in \mathfrak{b}$, luego $M_1, \dots, M_r \in \mathfrak{a} \cap \mathfrak{b}$.

(2).Dado un monomio $M \in \mathfrak{a} \cap \mathfrak{b}$, se tiene $M \in \mathfrak{a}$, luego existen monomios $A' \in K[X_1, \ldots, X_n]$ y A_i tales que $M = A'A_i$. como $M \in \mathfrak{b}$, existen monomios $B' \in K[X_1, \ldots, X_n]$ y B_j tales que $M = B'B_j$. entonces M es un múltiplo (monomial) de $M_{i,j}$.
(3).Representamos los m.c.m de los A_i y B_j en la siguiente tabla:

	$B_1 = X^3YZ$	$B_2 = X^2Y$	$B_3 = Y^2Z^3$
$A_1 = X$	$M_{1,1} = X^3YZ$	$M_{1,2} = X^2Y$	$M_{1,3} = XY^2Z^3$
$A_2 = Y^2Z$	$M_{1,2} = X^3Y^2Z$	$M_{2,2} = X^2Y^2Z$	$M_{2,3} = Y^2Z^3$
$A_3 = YZ^2$	$M_{1,3} = X^3YX^2$	$M_{3,2} = X^2YZ^2$	$M_{3,3} = Y^2Z^3$

El ideal intersección $\mathfrak{a} \cap \mathfrak{b}$ está generado por:

$$\{M_{1,1} = X^3YZ, M_{1,2} = X^2Y, M_{1,3} = XY^2Z^3, M_{2,1} = X^3Y^2Z, M_{2,2} = X^2Y^2Z,$$
$$M_{2,3} = Y^2Z^3, M_{3,1} = X^3YX^2, M_{3,2} = X^2YZ^2, M_{3,3} = Y^2Z^3\}$$

Esto es, $\mathfrak{a} \cap \mathfrak{b}$ es el ideal

$$(X^2Y, Y^2Z^3).$$

□

Lema de Dickson para ideales monomiales

Ejercicio. 16.19.
Sean $\mathfrak{a}_1$ y $\mathfrak{a}_2$ ideales monomiales con sistemas de generadores G_1 y G_2 respectivamente. Demuestra que:
(1) $\mathfrak{a}_1 + \mathfrak{a}_2$ está generado por $G_1 \cup G_2$,
(2) $\mathfrak{a}_1\mathfrak{a}_2$ está generado por $\{HL \mid H \in G_1, L \in G_2\}$.

Como consecuencia la suma y el producto de ideales monomiales es un ideal monomial.

SOLUCIÓN

Ejercicio. 16.20.
Demuestra que si $\{\mathfrak{a}_i \mid i \in I\}$ es una cadena de ideales monomiales, entonces la unión $\cup_i \mathfrak{a}_i$ es un ideal monomial.

SOLUCIÓN

Ejercicio. 16.21.
Demuestra que la intersección de ideales monomiales es un ideal monomial.

SOLUCIÓN

Ejercicio. 16.22.
Demuestra que si $\mathfrak{a}$ *y* $\mathfrak{b}$ *son ideales monomiales, entonces* $(\mathfrak{a} : \mathfrak{b})$ *es un ideal monomial.*

SOLUCIÓN

Ejercicio. 16.23.
Demuestra que:

(1) Un ideal monomial es primo si y solo si está generado por un subconjunto de$\{X_1, \ldots, X_n\}$
(2) El número de ideales monomiales primos es finito, y cada uno de ellos es finitamentegenerado.
(3) $(X_1, \ldots, X_n)$ *es el único ideal maximal que es monomial.*

SOLUCIÓN

Ejercicio. 16.24. (Lema de Dickson para ideales monomiales)
Todo ideal monomial en $K[X_1, \ldots, X_n]$ *es finitamente generado.*

SOLUCIÓN

Bases de Groebner

Ejercicio. 16.25.
Para cada $F \in K[X_1, \ldots, X_n]$ *se tiene* $\{\exp(F)\} + \mathbb{N}^n = \operatorname{Exp}(\operatorname{lm}(F)) = \operatorname{Exp}(F)$.
Este resultado no es cierto si el ideal no es principal.

SOLUCIÓN

Ejercicio. 16.26.
Da un ejemplo de dos polinomios F, $G \in K[X_1, \ldots, X_n]$ *tales que*$\operatorname{Exp}(F, G) \not\subseteq \{\exp F, \exp G\} + \mathbb{N}^n$.
Observar que la inclusioncontraria es siempre cierta.

SOLUCIÓN

Ejercicio. 16.27.
Sea $\mathfrak{a}$ un ideal monomial de $K[X_1,\dots,X_n]$ con generadores monomios $G_1,\dots,G_m$. Razona que $\{G_1,\dots,G_m\}$ es una base de Groebner de $\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 16.28.
Fijamos el orden lexicográfico $X > Y$ sobre $K[X,Y]$ y el ideal $\mathfrak{a} = (X^2Y - Y^2, X^3 - XY)$. Utiliza el criterio de Buchberger para mostrar que una base de Groebner de $\mathfrak{a}$ es $\{X^2Y - Y^2, X^3 - XY\}$. Estudia si $X^6 - X^5Y \in \mathfrak{a}$.

SOLUCIÓN

Ejercicio. 16.29.
Fijamos el orden lexicográfico $X > Y$ sobre $K[X,Y]$. Consideramos el ideal $\mathfrak{a} = (X - Y^3, X^2 - XY^2)$. Demuestra que la base de Groebner reducida de $\mathfrak{a}$ es $\{X - Y^3, Y^6 - Y^5)$.

SOLUCIÓN

Ejercicio. 16.30.
Sea $\mathfrak{a} = (Y - X^2, Z - X^3) \subseteq K[X,Y,Z]$.

(1) Demuestra que $\{Y - X^2, Z - X^3\}$ es una base de Groebner para el orden lexicográfico con $Z > Y > X$.
(2) Demuestra que $\{Y - X^2, Z - X^3\}$ no es una base de Groebner para el orden lexicográfico con $X > Z > Y$.

SOLUCIÓN

Ejercicio. 16.31.
Halla la base de Groebner reducida, con respecto al orden lexicográfico con $X > Y$, decada uno de los siguientes ideales de $K[X,Y]$:

(1) $\mathfrak{a} = (X^2 - 1, XY^2 - X)$,
(2) $\mathfrak{b} = (X^2 + Y, X^4 + 2X^2Y + Y^2 + 3)$.

SOLUCIÓN

Ejercicio. 16.32.
Se consideran los polinomios $F_1 = XY + X - 1$, $F_2 = X^2 + Y - 1$ en $K[X, Y]$. Determina una base de Groebner del ideal $\mathfrak{a} = (F_1, F_2)$ con respecto al orden lexicográfico (siendo $X > Y$).

SOLUCIÓN

Ejercicio. 16.33.
Se consideran los polinomios $F_1 = XY + X - 1$, $F_2 = X^2 + Y - 1$ en $K[X, Y]$. Determina una base de Groebner del ideal $\mathfrak{a} = (F_1, F_2)$ con respecto al orden lexicográfico (siendo $Y > X$).

SOLUCIÓN

Ejercicio. 16.34.
Cálculo de bases de Groebner.

(1) En $K[X, Y, Z]$ fijamos la ordenación lexicográfica con $X > Y > Z$. Determina una base de Groebner del ideal $\mathfrak{a} = (XZ, XY - Z, YZ - X)$. ¿El polinomio $X^3 + X + 1$ pertenece a $\mathfrak{a}$?
(2) En $K[X, Y]$ fijamos la ordenación lexicográfica con $X > Y$. Determina una base de Groebner del ideal $\mathfrak{b} = (X^2 - Y, Y^2 - X, X^2Y^2 - XY)$. ¿El polinomio $X^4 + X + 1$ pertenece a $\mathfrak{b}$?

SOLUCIÓN

Ejercicio. 16.35.
Fijamos el orden lexicográfico con $X > Y$ sobre $K[X, Y]$.

(1) Demuestra que la base de Groebner reducida del ideal $\mathfrak{a} = (X^3 - Y, X^2Y - Y^2)$ es $\{X^3 - Y, X^2Y - Y^2, XY^2 - Y^2, Y^3 - Y^2\}$.
(2) Determina si el polinomio $F = X^6 - X^5Y$ pertenece al ideal $\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 16.36.
Fijamos el orden lexicográfico con $X > Y > Z$ sobre $K[X, Y, Z]$. Demuestra que la base de Groebner reducida del ideal $\mathfrak{a} = (X^2 + XY + Z, XYZ + Z^2)$ es$\{X^2 + XY + Z, XYZ + Z^2, XZ^2, Z^3\}$. En particular deducir que el monoideal $\mathrm{Exp}(\mathfrak{a})$ requiere cuatro generadores.

SOLUCIÓN

Ejercicio. 16.37.
Sea el ideal $\mathfrak{a} = (X^2 - Y, X^2Y - Z) \subseteq K[X,Y,Z]$.

(1) Demuestra que $\{X^2 - Y, Y^2 - Z\}$ *es la base de Groebner reducida de* $\mathfrak{a}$ *respecto a la ordenación lexicográfica con* $X > Y > Z$.
(2) Demuestra que $\{X^2 - Y, Z - Y^2\}$ *es la base de Groebner reducida de* $\mathfrak{a}$ *respecto a la ordenación lexicográfica con* $Z > X > Y$. *(Observa que esencialmente son los mismos polinomios que en el apartado anterior.)*
(3) Demuestra que $\{Y - X^2, Z - X^4\}$ *es la base de Groebner reducida de* $\mathfrak{a}$ *respecto a la ordenación lexicográfica con* $Z > Y > X$.

SOLUCIÓN

Ejercicio. 16.38.
Sea $\mathfrak{a} = (XY + Y^2, X^2Y + XY^2 + X^2)$ *ideal de* $K[X,Y]$

(1) Demuestra que $\{X^2, XY + Y^2, Y^3\}$ *es la base de Groebner reducida de* $\mathfrak{a}$ *respecto a la ordenación lexicográfica* $X > Y$.
(2) Demuestra que $\{Y^2 + YX, X^2\}$ *es la base de Groebner reducida de* $\mathfrak{a}$ *respecto a la ordenación lexicográfica* $Y > X$.

(Observa que las bases tienen distinto número de elementos.)

SOLUCIÓN

Ejercicio. 16.39.
Consideramos el ideal $\mathfrak{a} = (H_1, H_2, H_3) \subseteq K[X,Y]$ *con*

$$\begin{aligned} H_1 &= X^2 + XY^5 + Y^4; \\ H_2 &= XY^6 - XY^3 + Y^5 - Y^2; \\ H_3 &= XY^5 - XY^2. \end{aligned}$$

(1) Demuestra que para el orden lexicográfico con $X > Y$ *la base de Groebner reducida de* $\mathfrak{a}$ *es* $\{X^2 + XY + Y^4, Y^5 - Y^2\}$
(2) Demuestra que para el orden lexicográfico graduado grlex *con* $X > Y$ *la base de Groebner reducida de* $\mathfrak{a}$ *es* $\{X^3 - Y^3, X^2 + XY^2 + Y^4, X^2Y + XY^3 + Y^2\}$

(Nótese que aunque el número de generadores es mayor, los grados son más pequeños.)

SOLUCIÓN

Ejercicio. 16.40.
Sea $\mathfrak{a} = (X^4 - Y^4 + Z^3 - 1, X^3 + Y^2 + Z^2 - 1) \subseteq K[X, Y, Z]$.

(1) Demuestra que hay cinco elementos en una base de Groebner reducida para $\mathfrak{a}$ *respecto al orden lexicográfico con* $X > Y > Z$. *(El grado máximo entre los cinco generadores es 12 y el número máximo de términos monomiales entre los cinco generadores es 35.)*
(2) Demuestra que hay dos elementos en una base de Groebner reducida para $\mathfrak{a}$ *respecto al orden lexicográfico con* $Y > Z > X$. *(El grado máximo es 6 y el número máximo de términos es 8)*
(3) Demuestra que para el orden invgrlex *la base de Groebner reducida de* $\mathfrak{a}$*es* $\{X^3 + Y^2 + Z^2 - 1, XY^2 + XZ^2 - X + Y^4 - Z^3 + 1\}$.

SOLUCIÓN

Ejercicio. 16.41.
Se considera los polinomios

$$G_1 = X^2YZ + Y^2Z + 1, G_2 = XY^2Z + YZ^2 - 2, G_3 = XYZ^2 + Z + 3 \in \mathbb{Q}[X, Y, Z],$$

y llamamos $\mathfrak{a}$ *al ideal generado por* G_1, G_2, G_3.

(1) Determina una base de Groebner del ideal $\mathfrak{a}$
(2) ¿Es $\{G_1, G_2, G_3\}$ *una base de Groebner de* $\mathfrak{a}$*?*
(3) Estudia si el polinomio $F = XYZ + 1$ *pertenece al ideal* $\mathfrak{a}$.
(4) Se consideran los polinomios $F_1 = 3X^2Z^9 + Z^{11} - 1, F_2 = Y^2Z^9 + 4Z^{12} + Z^8 - 5$. *Da los representantes canónicos de las clases de* F_1, F_2 *y* F_1F_2.
(5) ¿Cual es la dimensión del espacio vectorial $\mathbb{Q}[X, Y, Z]/\mathfrak{a}$*?*

SOLUCIÓN

Ejercicio. 16.42.
Determina una base de Groebner del ideal $\mathfrak{a}$ *generado por*$F = X^2 + Y^2 + Z^2 + XZ$,$G = X^4 + X4Y^2 + XZ^3 - Z^4 + 2$,$H = X^2 + XY - YZ + 3Y^2 - 4Z^2 - 1$*en los siguiente casos:*

(1) con el orden lexicográfico.
(2) con el orden lexicográfico graduado.
(3) con el orden lexicográfico graduado inverso.

SOLUCIÓN

Ejercicio. 16.43.
Se consideran los polinomios

$$F = X^2Y + 2XY^2 + 3Y^2$$
$$G = 2X^3Y - XY^3 + 1$$

(1) Calcula el resto de la división de$H = 2X^3Y^2 - 3X^3Y + 2X^2Y^2 - X^2Y - XY^4 + 2XY^3 + XY^2 - 3Y^2 + Y - 2$ por $\{F, G\}$. ¿Pertenece H al ideal generado por F y G?
(2) Calcula el resto de la división de$K = -2X^4Y + X^2Y^3 + X^2Y^2 - X^2Y + 2XY^3 - 2XY^2 - X + 3Y^3 - 3Y^2 + 1$ por $\{F, G\}F$. ¿Pertenece K al ideal generado por F y G?
(3) Calcula una base de Groebner del ideal generado por F y G.
(4) ¿Pertenecen H o K al ideal generado por F y G.

SOLUCIÓN

Aplicaciones de las bases de Groebner

Ejercicio. 16.44.
Demuestra que los ideales $\mathfrak{a} = (X^2Y + XY^2 - 2Y, X^2 + XY - X + Y^2 - 2Y, XY^2 - X - Y + Y^3)$,$\mathfrak{b} = (X - Y^2, XY - Y, X^2 - Y)$ *del anillo* $K[X, Y]$ *son iguales.*

SOLUCIÓN

Ejercicio. 16.45.
Demuestra que los ideales $\mathfrak{a} = (X^3 - YZ, YZ + Y)$, $\mathfrak{b} = (X^3Z + X^3, X^3 + Y)$ *de* $K[X, Y, Z]$ *son iguales.*

SOLUCIÓN

Ejercicio. 16.46.
Resuelve sobre $\mathbb{C}$ *el sistema de ecuaciones* $\begin{cases} X^2 - YZ = 3 \\ Y^2 - XZ = 4 \\ Z^2 - XY = 5 \end{cases}$

SOLUCIÓN

Ejercicio. 16.47.
Estudia los siguientes enunciados:

(1) Determina una base de Groebner del ideal $\mathfrak{a} = (X^2 + XY + Y^2 - 1, X^2 + 4Y^2 - 4) \subseteq \mathbb{R}[X, Y]$ *para el ordenlexicográfico con* $X > Y$.
(2) Halla en $\mathbb{R}^2$ *los cuatro puntos de intersección de la elipse* $X^2+XY+Y^2 = 1$ *con la elipse* $X^2+4Y^2 = 4$.

SOLUCIÓN

Ejercicio. 16.48.
Usa bases de Groebner para hallar las seis soluciones en $\mathbb{C}$ *del sistema deecuaciones*

$$\begin{cases} 2X^3 + 2X^2Y^2 + 3Y^3 = 0 \\ 3X^5 + 2X^3Y^3 + 2Y^5 = 0 \end{cases}$$

SOLUCIÓN

Ejercicio. 16.49.
Usa bases de Groebner para demostrar en $K[X, Y, Z]$ *que* $(X, Z) \cap (Y^2, X - YZ) = (XY, X - YZ)$.

SOLUCIÓN

Ejercicio. 16.50.
Usa bases de Groebner para determinar la intersección de los ideales de $K[X, Y]$.

$$\mathfrak{a} = (X^3Y - XY^2 + 1, X^2Y^2 - Y^3 - 1) \text{ y}$$
$$\mathfrak{b} = (X^2 - Y^2, X^3 + Y^3).$$

SOLUCIÓN

Ejercicio. 16.51.
Sean $\mathfrak{a} = (X^2Y + Z^3, X + Y^3 - Z, 2Y^4Z - YZ^2 - Z^3)$, $\mathfrak{b} = (X^2Y^5, X^3Z^4, Y^3Z^7)$*ideales de* $\mathbb{Q}[X, Y, Z]$. *Demuestra que* $(\mathfrak{a} : \mathfrak{b}) = (Z^2, Y + Z, X - Z)$.

SOLUCIÓN

Ejercicio. 16.52.
Sea A un anillo conmutativo, $\mathfrak{a} \supseteq \mathfrak{b}$ dos ideales de A y sea $\mathfrak{c}$ un ideal arbitrario de A. Sean $\overline{\mathfrak{a}} = \mathfrak{a}/\mathfrak{b}$, $\overline{\mathfrak{c}} = (\mathfrak{c}+\mathfrak{b})/\mathfrak{b}$, $\overline{(\mathfrak{a}:\mathfrak{c})} = ((\mathfrak{a}:\mathfrak{c})+\mathfrak{b})/\mathfrak{b}$ los ideales correspondientes del anillo cociente $A/\mathfrak{b}$. Demuestra que $\overline{(\mathfrak{a}:\mathfrak{c})} = (\overline{\mathfrak{a}}:\overline{\mathfrak{c}})$.

SOLUCIÓN

Ejercicio. 16.53.
Sea $\mathfrak{b} = (Y^5 - Z^4) \subseteq A = \mathbb{Q}[Y,Z]$. Para cada uno de los siguientes pares de ideales $\mathfrak{a}$, $\mathfrak{c}$ comprobar que $(\overline{\mathfrak{a}}:\overline{\mathfrak{c}})$ es el ideal de $A/\mathfrak{b}$ citado:

(1) $\mathfrak{a} = (Y^3, Y^5 - Z^4)$, $\mathfrak{c} = (Z)$, $(\overline{\mathfrak{a}}:\overline{\mathfrak{c}}) = (\overline{Y}^3, \overline{Z}^3)$.
(2) $\mathfrak{a} = (Y^3, Z, Y^4 - Z^4)$, $\mathfrak{c} = (Y)$, $(\overline{\mathfrak{a}}:\overline{\mathfrak{c}}) = (\overline{Y}^2, \overline{Z})$.
(3) $\mathfrak{a} = (Y, Y^3, Z, Y^5 - Z^4)$, $\mathfrak{c} = (1)$, $(\overline{\mathfrak{a}}:\overline{\mathfrak{c}}) = (\overline{Y}, \overline{Z})$.

SOLUCIÓN

Ejercicio. 16.54.
Determina los siguientes ideales:

(1) $\mathfrak{a} = (X,Y,Z) \cap (X-1, Y-1, Z-1) \cap (X+1, Y+1, Z+1)$.
(2) $\mathfrak{b} = (\mathfrak{a} : XYZ)$.
(3) $\mathfrak{c} = (\mathfrak{a} : X^3Y^2Z)$.

SOLUCIÓN

Ejercicio. 16.55.
Determina la suma y la intersección de los siguientes ideales:

$$\mathfrak{a} = (X + Y^2 + Y + 1, X - Z^2 + Z - 1),$$
$$\mathfrak{b} = (XY - YZ + 1, Y^2 + Y - 1).$$

SOLUCIÓN

Ejercicio. 16.56.
Calcula la intersección y la unión de las dos superficies

$$\{(x,y,z) \mid\ 1+x^2+y^2-z\} \quad y \quad \{(x,y,z) \mid\ x^4+2x^2y^2+y^4-4x^3z+12xy^2z\}.$$

SOLUCIÓN

Capítulo III

Conjuntos algebraicos afines

Introducción

El objetivo de este capítulo es estudiar objetos geométricos definidos como conjuntos de ceros de sistemas de ecuaciones polinómicas (los conjuntos algebraicos afines). Establecemos una correspondencia de Galois entre conjuntos algebraicos en el espacio afín $\mathbb{A}^n(K)$ e ideales del anillo de polinomios $K[X_1, \ldots, X_n]$. A continuación a cada conjunto algebraico afín V le asociamos su anillo de coordenadas, $K[V] = K[X_1, \ldots, X_n]/\mathcal{I}(V)$, siendo $\mathcal{I}(V)$ el ideal de todos los polinomios que se anulan en todos los puntos de V, y estudiamos propiedades (geométricas) de V en función de propiedades (algebraicas) de $K[V]$, y viceversa.

Se introducen las aplicaciones polinómicas entre dos conjuntos algebraicos V y W y se relaciones con los homomorfismos de álgebras de $K[W]$ a $K[V]$. Finalmente, haciendo uso de la teoría de bases de Groebner se clasifican los homomorfismos de álgebras entre dos anillos coordenados.

17. Funciones polinómicas

Sea K un cuerpo, para cada $n \in \mathbb{N} \setminus \{0\}$ consideramos K^n, el producto cartesiano de n copias de K. En K^n podemos considerar una estructura de espacio afín, a la que vamos a representar por $\mathbb{A}^n(K)$, o simplemente por $\mathbb{A}^n$ o $\mathbb{A}$.

En un espacio afín $\mathbb{A}^n$ tenemos **puntos**, los elementos de $\mathbb{A}^n$, **hiperplanos**, los conjuntos de ceros de las formas lineales, y las **variedades lineales afines**, la intersecciones de hiperplanos, o los conjuntos de ceros de conjuntos de formas lineales.

La estructura de espacio afín se puede enriquecer aún más, y en nuestro caso vamos a ver como los polinomios proporcionan una estructura geométrica adicional a cada espacio afín.

Dado el espacio $\mathbb{A}^n(K)$ y un polinomio $F \in K[X_1,\ldots,X_n]$, definimos una **función polinómica** $F^* : \mathbb{A}^n(K) \longrightarrow K$ mediante $F^*(x_1,\ldots,x_n) = F(x_1,\ldots,x_n)$ para cada $(x_1,\ldots,x_n) \in \mathbb{A}^n(K)$.

Observar que dos polinomios distintos pueden definir la misma función polinómica. Este es el caso de $X(X-1)$ y $0 \in \mathbb{F}_2[X]$, que definen la función constante igual a 0 en $\mathbb{A}^1(\mathbb{F}_2)$.

Llamamos $\mathcal{P}(\mathbb{A}^n(K))$ al conjunto de las funciones polinómicas. En $\mathcal{P}(\mathbb{A}^n(K))$ podemos definir una estructura de K–álgebra mediante las operaciones:

$$\left.\begin{array}{l}(f+g)(x_1,\ldots,x_n) = f(x_1,\ldots,x_n) + g(x_1,\ldots,x_n),\\ (f\cdot g)(x_1,\ldots,x_n) = f(x_1,\ldots,x_n)\cdot g(x_1,\ldots,x_n),\\ (k\cdot f)(x_1,\ldots,x_n) = k\cdot f(x_1,\ldots,x_n),\end{array}\right\} \quad \begin{array}{l}\forall f,g \in \mathcal{P}(\mathbb{A}^n(K)),\\ \forall k \in K,\\ \forall (x_1,\ldots,x_n) \in \mathbb{A}^n(K).\end{array}$$

Tenemos entonces una aplicación de K–álgebras $(-)^* : K[X_1,\ldots,X_n] \longrightarrow \mathcal{P}(\mathbb{A}^n(K))$, $F \mapsto F^*$.

Proposición. 17.1.
La aplicación $(-)^*$ es un homomorfismo sobreyectivo de K–álgebras y es un isomorfismo si, y solo si, K es un cuerpo infinito.

Llamamos a $\mathcal{P}(\mathbb{A}^n(K))$ el **anillo de coordenadas** de $\mathbb{A}^n(K)$, y lo representaremos por $K[\mathbb{A}^n]$.

18. Conjuntos algebraicos afines

La estructura adicional de $\mathbb{A}^n(K)$ al considerar las funciones polinómicas nos permite considerar los conjuntos de ceros de estas funciones. Debido a la existencia de la aplicación sobreyectiva $(-)^* : K[X_1,\ldots,X_n] \longrightarrow K[\mathbb{A}^n]$, al estudiar el conjunto de ceros de una función polinómica F^* podemos identificar este conjunto con el conjunto de raíces, en K^n, del polinomio F, identificando a este fin los conjuntos $\mathbb{A}^n(K)$ y K^n.
Cada polinomio $F \in K[X_1,\ldots,X_n]$ determina un subconjunto

$$\mathcal{V}(F) = \{(x_1,\ldots,x_n) \in \mathbb{A}^n(K) \mid F(x_1,\ldots,x_n) = 0\},$$

el **conjunto de ceros** o **conjunto de raíces** de F^* ó F. Para cada conjunto $\mathcal{F} \subseteq K[X_1,\ldots,X_n]$ podemos considerar

$$\mathcal{V}(\mathcal{F}) = \cap\{\mathcal{V}(F) \subseteq \mathbb{A}^n(K) \mid F \in \mathcal{F}\},$$

el conjunto de ceros comunes a todos los elementos de $\mathcal{F}$.
Un subconjunto $V \subseteq \mathbb{A}^n(K)$ se llama un **conjunto algebraico afín** si existe un conjunto de polinomios $\mathcal{F} \subseteq K[X_1,\ldots,X_n]$ tal que $V = \mathcal{V}(\mathcal{F})$.

Lema. 18.1.
Si $\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq K[X_1,\ldots,X_n]$ son conjuntos de polinomios, entonces $\mathcal{V}(\mathcal{F}_1) \supseteq \mathcal{V}(\mathcal{F}_2)$.

Lema. 18.2.
Sean $\mathcal{F} \subseteq K[X_1,\ldots,X_n]$ un conjunto de polinomios y $\mathfrak{a}$ el ideal generado por $\mathcal{F}$. Se verifica:
(1) $\mathcal{V}(\mathcal{F}) = \mathcal{V}(\mathfrak{a})$.
(2) Existen polinomios $F_1,\ldots,F_s \in \mathcal{F}$ tales que $\mathcal{V}(\mathcal{F}) = \mathcal{V}(F_1,\ldots,F_s)$.

Proposición. 18.3.
(1) Si V_1 y V_2 son conjuntos algebraicos afines de $\mathbb{A}^n(K)$, entonces $V_1 \cup V_2$ es un conjunto algebraico afín.
(2) Si $\{V_i \mid i \in I\}$ es una familia de conjuntos algebraicos afines de $\mathbb{A}^n(K)$, entonces $\cap_i V_i$ es un conjunto algebraico afín.

Como consecuencia los conjuntos algebraicos afines verifican los axiomas de los cerrados para una topología en $\mathbb{A}^n$. Esta topología se llama la **topología de Zariski** de $\mathbb{A}^n(K)$. Los conjuntos algebraicos afines verifican las siguientes propiedades:

(I) $\varnothing$ y $\mathbb{A}^n$ son conjuntos algebraicos.

(II) La unión finita de conjuntos algebraicos afines es un conjunto algebraico afín.

(III) La intersección de conjuntos algebraicos afines es un conjunto algebraico afín.

Ejemplos. 18.4.

(1) **Puntos.** Observar que $\mathcal{V}(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$, y por lo tanto tenemos que cada conjunto finito es un cerrado, esto es, un conjunto algebraico afín.

(2) **Conjuntos lineales.** Son los conjuntos de ceros de los sistemas de ecuaciones lineales.

(3) **Hipersuperficies.** Son los conjuntos de ceros de polinomios $F \in K[X_1, \ldots, X_n]$ no constantes. Es claro que todo conjunto algebraico afín es una intersección de un número finito de hipersuperficies.

(4) **Hiperplanos.** Son los conjuntos de ceros de polinomios de grado uno. Cada conjunto lineal es una intersección finita de hiperplanos.

Las propiedades de los conjuntos algebraicos afines pueden expresarse también en términos de ideales como sigue:

Lema. 18.5. (Propiedades de los conjuntos algebraicos afines.)

(1) Para cada familia de ideales $\{\mathfrak{a}_i \mid i \in I\}$ *en* $K[X_1, \ldots, X_n]$ *se tiene* $\mathcal{V}(\sum_i \mathfrak{a}_i) = \cap_i \mathcal{V}(\mathfrak{a}_i)$;

(2) Si $\mathfrak{a} \subseteq \mathfrak{b}$, *entonces* $\mathcal{V}(\mathfrak{a}) \supseteq \mathcal{V}(\mathfrak{b})$;

(3) $\mathcal{V}(FG) = \mathcal{V}(F) \cup \mathcal{V}(G)$, *para* $F, G \in K[X_1, \ldots, X_n]$,
$\mathcal{V}(\mathfrak{a}\mathfrak{b}) = \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}) = \mathcal{V}(\mathfrak{a} \cap \mathfrak{b})$, *para* $\mathfrak{a}, \mathfrak{b} \subseteq K[X_1, \ldots, X_n]$;

(4) $\mathcal{V}(0) = \mathbb{A}^n$,
$\mathcal{V}(1) = \varnothing$.

19. Ideales asociados a conjuntos de puntos

Dado un conjunto de puntos $\mathcal{S} \subseteq \mathbb{A}^n$, llamamos **ideal** de $\mathcal{S}$ al conjunto

$$\mathcal{I}(\mathcal{S}) = \{F \in K[X_1, \ldots, X_n] \mid F(s) = 0, \text{ para cada } s \in \mathcal{S}\}.$$

Veamos ahora algunas de las propiedades de los operadores $\mathcal{I}$ y $\mathcal{V}$.

Lema. 19.1.
(1) Si $\mathcal{S}_1 \subseteq \mathcal{S}_2$, entonces $\mathcal{I}(\mathcal{S}_1) \supseteq \mathcal{I}(\mathcal{S}_2)$.
(2) $\mathcal{I}(\varnothing) = K[X_1, \ldots, X_n]$,
$\mathcal{I}(\mathbb{A}^n) = 0$, si K es un cuerpo infinito.
(3) $\mathcal{F} \subseteq \mathcal{IV}(\mathcal{F})$ para cada conjunto de polinomios $\mathcal{F} \subseteq K[X_1, \ldots, X_n]$,
$\mathcal{S} \subseteq \mathcal{VI}(\mathcal{S})$ para cada conjunto de puntos $\mathcal{S} \subseteq \mathbb{A}^n$.
(4) $\mathcal{V}(\mathcal{F}) = \mathcal{VIV}(\mathcal{F})$ para cada conjunto de polinomios $\mathcal{F} \subseteq K[X_1, \ldots, X_n]$,
$\mathcal{I}(\mathcal{S}) = \mathcal{IVI}(\mathcal{S})$ para cada conjunto de puntos $\mathcal{S} \subseteq \mathbb{A}^n$.
(5) $\mathcal{I}(\mathcal{S})$ es un ideal radical para cada conjunto de puntos $\mathcal{S} \subseteq \mathbb{A}^n$.

DEMOSTRACIÓN. (5). Se tiene $F \in \mathcal{I}(\mathcal{S})$ si y solo si, para cada $x \in \mathcal{S}$ ocurre que $F(x) = 0$. Dado $G \in K[X_1, \ldots, X_n]$ tal que existe $m \in \mathbb{N}$ verificando $G^m \in \mathcal{I}(\mathcal{S})$, entonces $0 = G^m(x) = G(x)^m$, y por tanto $G(x) = 0$, esto es, $G \in \mathcal{I}(\mathcal{S})$, que por tanto es un ideal radical. □

La demostración del siguiente hecho requiere de un estudio más avanzado de los conjuntos algebraicos afines, y en concreto del Teorema de los ceros de Hilbert, ver Teorema (37.3.), por lo que lo citamos solamente a modo de ejemplo.

Corolario. 19.2.
Dado un ideal $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$, resulta que $\mathcal{IV}(\mathfrak{a}) = \operatorname{rad}(\mathfrak{a})$.

Como consecuencia, si V es un conjunto algebraico, entonces $V = \mathcal{VI}(V)$, y si $\mathfrak{a}$ es el ideal de un conjunto de puntos $\mathfrak{a} = \mathcal{IV}(\mathfrak{a})$. Más adelante veremos cual es el marco más adecuado en el que establecer una biyección entre conjuntos algebraicos afines de $\mathbb{A}^n(K)$ y ciertos ideales del anillo $K[X_1, \ldots, X_n]$.

Ejercicio. 19.3.
(1) Si V_1, V_2 son conjuntos algebraicos afines, entonces:

$$V_1 \subseteq V_2 \;\Leftrightarrow\; \mathcal{I}(V_1) \supseteq \mathcal{I}(V_2);$$

$$V_1 \subset V_2 \;\Leftrightarrow\; \mathcal{I}(V_1) \supset \mathcal{I}(V_2);$$

(2) Si V_1 y V_2 son conjuntos algebraicos afines, entonces:

$$\mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2);$$

$$V_1 \cup V_2 = \mathcal{V}(\mathcal{I}(V_1)\mathcal{I}(V_2)) = \mathcal{V}(\mathcal{I}(V_1) \cap \mathcal{I}(V_2)).$$

(3) Si $\{V_\alpha \mid \alpha \in A\}$ es una familia de conjuntos algebraicos afines, entonces

$$\cap_\alpha V_\alpha = \mathcal{V}(\sum_\alpha \mathcal{I}(V_\alpha)).$$

Vamos a calcular algunos ejemplos.

Ejemplo. 19.4.
Si K es un cuerpo de característica cero y $\mathcal{S} = \{(x_1, \ldots, x_n)\}$ es un conjunto de K^n que se reduce a un punto, entonces $\mathcal{I}(x_1, \ldots, x_n) = (X_1 - x_1, \ldots, X_n - x_n)$, que es un ideal maximal de $K[X_1, \ldots, X_n]$.

Ejemplo. 19.5.
Si K es un cuerpo de característica cero y $\mathcal{S}$ es el conjunto de los ceros de $X^3 - Y^2$, vamos a determinar $\mathcal{I}(\mathcal{S}) = \mathcal{I}\mathcal{V}(X^3 - Y^2)$.

En este caso podemos dar una parametrización de este conjunto algebraico. Dado un cero $(x, y) \neq (0, 0)$, resulta $x^3 = y^2$, y por lo tanto se tiene $x = \left(\frac{y}{x}\right)^2$ e $y = \left(\frac{y}{x}\right)^3$. Si llamamos $t = \frac{y}{x}$, entonces se tiene $x = t^2$, $y = t^3$. Como consecuencia el conjunto de ceros es: $\{(t^2, t^3) \mid t \in K\}$.

Para determinar el ideal $\mathfrak{a} = \mathcal{I}(\mathcal{V}(X^3 - Y^2))$, basta ver que si $F \in \mathfrak{a}$, al dividir por $X^3 - Y^2$, consideramos el orden lexicográfico con $Y > X$, entonces $F = (X^3 - Y^2)Q + R$, con $R = 0$ ó $\mathcal{N}(R) \subseteq \overline{\Delta} = \mathbb{N}^2 \setminus ((0, 2) + \mathbb{N}^2)$. Para cada $t \in K$ se tiene $F(t^2, t^3) = 0$, luego $R(t^2, t^3) = 0$, y el polinomio $R(T^2, T^3) \in K[T]$ tiene como raíces a todos los elementos de K. Como K es infinito, entonces $R(T^2, T^3)$ es el polinomio cero; observar que $R(X, Y) = R_0(X) + YR_1(X)$, y que por tanto se tiene $0 = R_0(T^2) + T^3R_1(T^2)$. De aquí se deduce que $R_0 = 0$ y $R_1 = 0$ y por tanto $R = 0$, esto es, $F = (X^3 - Y^2)Q \in (X^3 - Y^2)$ y $\mathcal{I}\mathcal{V}(X^3 - Y^2) = (X^3 - Y^2)$.

Si K no es de característica cero, este resultado puede no ser cierto. Observar el caso en que $K = \mathbb{F}_2$, entonces $\mathcal{V}(X^3 - Y^2) = \{(0, 0), (1, 1)\}$, y se tiene $\mathcal{I}\mathcal{V}(X^3 - Y^2) = (X, Y) \cap (X - 1, Y - 1) = (X + Y, Y^2 + Y)$.

20. Anillos coordenados

Recordemos que dado un conjunto algebraico afín $V \subseteq \mathbb{A}^n(K)$, el anillo $K[V] := K[X_1, \ldots, X_n]/\mathcal{I}(V)$ se llama el **anillo coordenado** de V.

Dadas dos funciones polinómicas F^*, G^* sobre $\mathbb{A}^n(K)$, podemos considerar sus restricciones a $V \subseteq \mathbb{A}^n(K)$. Observar que si $F^*_{|V} = G^*_{|V}$, entonces para cada $v \in V$ se tiene $F(v) = G(v)$, esto es, $F - G \in \mathcal{I}(V)$. Y recíprocamente. Tenemos pues una biyección entre $K[V]$ y las clases de equivalencia, para la relación $F^* \sim G^*$ si $F^*_{|V} = G^*_{|V}$, de las funciones polinómicas, por lo que podemos identificar los elementos de $K[V]$ con funciones polinómicas sobre V.

Ejemplo. 20.1.
Si consideramos $\mathcal{V}(X^3 - Y^2)$, como en el ejemplo (19.5.). En el caso en que K es un cuerpo de característica cero se tiene $\mathcal{I}(\mathcal{V}(X^3 - Y^2)) = (X^3 - Y^2)$, y por tanto $K[\mathcal{V}(X^3 - Y^2)] = K[X, Y]/(X^3 - Y^2)$. Sin embargo si $K = \mathbb{F}_2$, entonces $\mathbb{F}_2[\mathcal{V}(X^3 - Y^2)] = \mathbb{F}_2[X, Y]/(X + Y, Y^2 + Y) \cong \mathbb{F}_2[Y]/(Y^2 + Y) \cong \mathbb{F}_2 \times \mathbb{F}_2$.

Dados dos conjuntos algebraicos afines $V \subseteq \mathbb{A}^n(K)$ y $W \subseteq \mathbb{A}^m(K)$. Vamos a llamar **aplicación polinómica**, **morfismo de conjuntos afines** o **aplicación regular** de V a W a una aplicación $f : V \longrightarrow W$ definida por polinomios, esto es, para cada índice $j = 1, \ldots, m$ existe un polinomio $F_j \in K[X_1, \ldots, X_n]$ tal que

$$f(x_1, \ldots, x_n) = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) \quad \text{para cada } (x_1, \ldots, x_n) \in V.$$

Observar que los polinomios F_j no están determinados de forma única. Por ejemplo si $V = \mathcal{V}(X^2 + Y^2 - 1) \subseteq \mathbb{A}^2(\mathbb{R})$, los polinomios $F = X$ y $G = X + X^2 + Y^2 - 1$ definen la misma aplicación polinómica de V a $\mathbb{A}^1(\mathbb{R})$.

Una aplicación polinómica $f : V \longrightarrow W$ se dice que es un **isomorfismo** de conjuntos algebraicos afines si existe otra aplicación polinómica $g : W \longrightarrow V$ tal que $f \circ g = \mathrm{id}_W$ y $g \circ f = \mathrm{id}_V$.

Proposición. 20.2.
Sean $V \subseteq \mathbb{A}^n(K)$ y $W \subseteq \mathbb{A}^m(K)$ conjuntos algebraicos afines. Se verifica:

(1) Toda aplicación polinómica $f : V \longrightarrow W$ define un homomorfismo de K–álgebras

$$\widetilde{f} : K[W] \longrightarrow K[V], \quad \widetilde{f}(\overline{F}) = \overline{F} \circ f.$$

(2) Para cada homomorfismo de K–álgebras $h : K[W] \longrightarrow K[V]$ existe una única aplicación polinómica $f : V \longrightarrow W$ tal que $h = \widetilde{f}$.

(3) Si $f_1 : V_1 \longrightarrow V_2$ y $f_2 : V_2 \longrightarrow V_3$ son aplicaciones polinómicas, entonces $\widetilde{f_2 \circ f_1} = \widetilde{f_1} \circ \widetilde{f_2}$.

(4) Una aplicación polinómica $f : V \longrightarrow W$ es un isomorfismo si, y solo si, $\widetilde{f}$ es un isomorfismo de K–álgebras.

DEMOSTRACIÓN. (2). Dado $h : K[W] \longrightarrow K[V]$, para cada índice $j = 1, \ldots, m$ definimos $\overline{F_j} = h(\overline{Y_j})$. Y juntándolos todos definimos una aplicación polinómica $h' : V \longrightarrow \mathbb{A}^m(K)$ mediante:

$$h'(x_1, \ldots, x_n) = (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)), \quad \text{para cada } (x_1, \ldots, x_n) \in V.$$

Ahora comprobamos que $h'(V) \subseteq W$, para esto consideramos el diagrama

$$\begin{array}{ccccc} \mathcal{I}(W) & \longrightarrow & K[Y_1, \ldots, Y_m] & \longrightarrow & K[W] \\ \downarrow{\scriptstyle h''} & & \downarrow{\scriptstyle h'} & & \downarrow{\scriptstyle h} \\ \mathcal{I}(V) & \longrightarrow & K[X_1, \ldots, X_n] & \longrightarrow & K[V] \end{array}$$

donde $h' : K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n]$ está definido $h'(Y_j) = F_j$, para cada índice j. Es claro que $h'(\mathcal{I}(W)) \subseteq \mathcal{I}(V)$, lo que permite definir h''.
Observar que si $G \in \mathcal{I}(W)$, y $(x_1, \ldots, x_n) \in V$, entonces

$$0 = h''(G)(x_1, \ldots, x_n) = G(F_1, \ldots, F_m)(x_1, \ldots, x_n) = G(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n))),$$

y para cada $(x_1, \ldots, x_n) \in V$ se tiene $(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)) \in W$. Por tanto h' define una aplicación polinómica de V a W.
Podemos observar que si se eligen otros elementos F'_j tales que $\overline{F_j} = \overline{F'_j}$ para cada índice $j = 1, \ldots, m$, entonces $\overline{F_j} = \overline{F'_j}$, como funciones polinómicas, por lo tanto podemos tomar tanto una como la otra en la definición de la aplicación polinómica $h' : V \longrightarrow W$.
Finalmente observar que $\widetilde{h'} = h$, ya que para cada $\overline{G} \in K[W]$ se tiene:

$$\widetilde{h'}(\overline{G}) = \overline{G \circ h'} = \overline{G(F_1, \ldots, F_m)} = h(\overline{G}).$$

□

Como consecuencia de la proposición, existe una biyección:

$$\mathrm{Hom}_{Apl.Pol.}(V, W) \xrightarrow{\cong} \mathrm{Hom}_{K-Alg.}(K[W], K[V]).$$

Corolario. 20.3.
Sea $f : V \longrightarrow W$ una aplicación entre conjuntos algebraicos afines. Son equivalentes:
(a) f es una aplicación polinómica.
(b) Para cada $g \in K[W]$ la composición $g \circ f$ pertenece a $K[V]$.

En particular, para cada aplicación polinómica $f : V \longrightarrow W$ se tiene $f(v) = w$ si, y solo si, $\widetilde{f}^{-1}(\mathcal{I}(\{v\})) = \mathcal{I}(\{w\})$.

DEMOSTRACIÓN. (a) ⇒ (b). Tenemos $\widetilde{f}(g) = g \circ f \in K[V]$ para cada $g \in K[W]$.
(b) ⇒ (a). Para cada índice $j = 1, \ldots, m$ tomamos $\overline{X_j} \in K[W]$, por hipótesis $\overline{X_j} \circ f \in K[V]$, luego existe un polinomio $F_j \in K[X_1, \ldots, X_n]$ tal que $\overline{F_j} = \overline{X_j} \circ f$. Es claro que $f(v) = (F_1(v), \ldots, F_m(v))$ para cada $v \in V$.
La segunda parte es clara. □

Ejemplo. 20.4.
Vamos a ver que existe una aplicación polinómica biyectiva entre $\mathcal{V}(X^3 - Y^2) \subseteq \mathbb{R}^2$ y la recta afín real que no es un isomorfismo.
Tenemos una parametrización de $\mathcal{V}(X^3 - Y^2)$ dada por $x = t^2$, $y = t^3$, donde t varía en $\mathbb{R}$. Definimos entonces

$$f : \mathbb{A}^1(\mathbb{R}) \longrightarrow \mathcal{V}(X^3 - Y^2),$$

mediante: $f(t) = (t^2, t^3)$, $t \in \mathbb{R}$. Es claro que f es una aplicación de conjuntos algebraicos y es biyectiva, pero vamos a ver que no es un isomorfismo. Al considerar el homomorfismo inducido

$$\widetilde{f} : K[\mathcal{V}(X^3 - Y^2)] \longrightarrow K[\mathbb{A}^1(\mathbb{R})],$$

se tiene

$$\widetilde{f} : \frac{\mathbb{R}[X, Y]}{(X^3 - Y^2)} \longrightarrow \mathbb{R}[T], \quad \widetilde{f}(X) = T^2, \quad \widetilde{f}(Y) = T^3.$$

Por lo tanto la imagen es el subanillo generado por T^2 y T^3, esto es, $\mathbb{R} + T^2\mathbb{R}[T] \neq \mathbb{R}[T]$, y como no es un isomorfismo, tenemos que f no es un isomorfismo de conjuntos algebraicos.
Más adelante veremos que en realidad no puede existir ningún isomorfismo entre $\mathcal{V}(X^3 - Y^2)$ y la recta afín real.

Homomorfismos de álgebras afines

En lo que sigue vamos a estudiar los homomorfismos $h : K[W] \longrightarrow K[V]$ determinando su núcleo y su imagen. Supongamos que

$$h : \frac{K[Y_1, \ldots, Y_m]}{\mathcal{I}(W)} \longrightarrow \frac{K[X_1, \ldots, X_n]}{\mathcal{I}(V)}.$$

Para cada elección de $F_1, \ldots, F_m \in K[X_1, \ldots, X_n]$ tenemos un homomorfismo

$$g : K[Y_1, \ldots, Y_m] \longrightarrow K[X_1, \ldots, X_n], \quad g(Y_j) = F_j,\ j = 1, \ldots, m.$$

Además g induce un homomorfismo de $K[W]$ a $K[V]$ si $g(\mathcal{I}(W)) \subseteq \mathcal{I}(V)$, esto es, si para cada $G \in \mathcal{I}(W)$ se tiene $G(F_1, \ldots, F_m) \in \mathcal{I}(V)$.
Entonces el homomorfismo h estará determinado por las imágenes de $\overline{Y_j}$, $j = 1, \ldots, m$. Sean $F_j \in K[X_1, \ldots, X_n]$ tales que $\overline{F_j} = h(\overline{Y_j})$. Los F_j están determinados módulo $\mathcal{I}(V)$, pero para cualquier elección de estos se tiene el mismo valor, $h(\overline{G}) = \overline{G(F_1, \ldots, F_m)}$.

Proposición. 20.5.
Sean $A = K[Y_1,\ldots,Y_m,X_1,\ldots,X_n]$, $\mathfrak{c}$ *el ideal de* A *generado por* $\{Y_1 - F_1,\ldots,Y_m - F_m\} \cup \{$*sistema de generadores de* $\mathcal{I}(V)\}$ *y sea* $\mathbb{G}$ *la base de Groebner reducida de* $\mathfrak{c}$ *con respecto al orden lexicográfico con* $X_1 > \cdots > X_n > Y_1 > \cdots > Y_m$. *Se tiene:*

(1) $\operatorname{Ker}(h) = \dfrac{(\mathfrak{c}\cap K[Y_1,\ldots,Y_m]) + \mathcal{I}(W)}{\mathcal{I}(W)}$. *En particular las clases de los elementos de* $\mathbb{G}$ *en* $K[X_1,\ldots,X_n]$ *generan* $\operatorname{Ker}(h)$.
(2) Dado $F \in K[X_1,\ldots,X_n]$, *se tiene* $\overline{F} \in \operatorname{Im}(h)$ *si, y solo si,* $R(F;\mathbb{G}) \in K[Y_1,\ldots,Y_m]$. *En este caso* $\overline{F} = h(\overline{R(F;\mathbb{G})})$.

DEMOSTRACIÓN. (1). Si $\overline{G} \in \operatorname{Ker}(h)$, entonces $0 = h(\overline{G}) = \overline{G(F_1,\ldots,F_m)}$, y por tanto tenemos $G(F_1,\ldots,F_m) \in \mathcal{I}(V)$, luego $G(F_1,\ldots,F_m) \in \mathcal{I}(V)^e \subseteq \mathfrak{c}$. Como $Y_j - F_j \in \mathfrak{c}$ para cada $j = 1,\ldots,m$, entonces $G(Y_1,\ldots,Y_m) - G(F_1,\ldots,F_m) \in \mathfrak{c}$, y tenemos $G \in \mathfrak{c}\cap K[Y_1,\ldots,Y_m]$, luego $\overline{G} \in \dfrac{(\mathfrak{c}\cap K[Y_1,\ldots,Y_m]) + \mathcal{I}(W)}{\mathcal{I}(W)}$.
Por otro lado, si $G \in \mathfrak{c}\cap K[Y_1,\ldots,Y_m]$, supongamos que $\mathcal{I}(V)$ está generado por $\{H_1,\ldots,H_t\}$, entonces

$$G(Y_1,\ldots,Y_m) = \sum_{j=1}^{m} a_j(Y_j - F_j) + \sum_{i=1}^{t} b_iH_i,$$

con $a_j, b_i \in A$. Tenemos $G(F_1,\ldots,F_m) = \sum_{i=1}^{t} b_iH_i \in \mathcal{I}(V)^e$, y por tanto $h(\overline{G}) = \overline{G(F_1,\ldots,F_m)} = 0$.
(2). Dado $F \in K[X_1,\ldots,X_n]$, si $\overline{F} \in \operatorname{Im}(h)$, entonces existe $G \in K[Y_1,\ldots,Y_m]$ tal que $h(\overline{G}) = \overline{F}$, y por tanto $G(F_1,\ldots,F_m) - F(X_1,\ldots,X_n) \in \mathcal{I}(V) \subseteq \mathfrak{c}$. Como $G(F_1,\ldots,F_m) - G(Y_1,\ldots,Y_m) \in \mathfrak{c}$, tenemos $G(Y_1,\ldots,Y_m) - F(X_1,\ldots,X_n) \in \mathfrak{c}$. Al hacer la división de F, ó de G, por $\mathbb{G}$, como $X_1 > \cdots > X_n > Y_1 > \cdots > Y_m$ en el orden lexicográfico, en el resto R no aparecen las variables $X_1,\ldots,X_n$, luego $G - R \in \mathfrak{c}\cap K[Y_1,\ldots,Y_m]$, y como sus clases están contenidas en el núcleo, entonces $\overline{F} = h(\overline{G}) = h(\overline{R})$.
Por otro lado, sea $R \in K[Y_1,\ldots,Y_m]$ el resto de la división de F por $\mathbb{G}$, entonces $F - R \in \mathfrak{c}$ y podemos escribir

$$F - R = \sum_{j=1}^{m} a_j(Y_j - F_j) + \sum_{i=1}^{t} b_iH_i.$$

Al evaluar Y_j en F_j resulta $F - R(F_1,\ldots,F_m) = \sum_{i=1}^{t} b_iH_i \in \mathcal{I}(V)$. Entonces $\overline{F} = h(\overline{R}) \in \operatorname{Im}(h)$. □

Corolario. 20.6.
(1) h *es inyectiva si, y solo si,* $\mathfrak{c}\cap K[Y_1,\ldots,Y_m] \subseteq \mathcal{I}(W)$.
(2) h *es sobreyectiva si, y solo si, para cada índice* $i = 1,\ldots,n$ *existe un* $G_i \in K[Y_1,\ldots,Y_m]$ *tal que* $X_i - G_i \in \mathbb{G}$.

DEMOSTRACIÓN. (1). Es inmediata.

(2). Es claro que la condición es necesaria, ya que para cada índice i se tendrá $R(X_i;\mathbb{G}) \in K[Y_1,\ldots,Y_m]$ y por tanto $\overline{X_i}$ pertenece a la imagen de h. Por otro lado, si h es sobreyectiva, entonces para cada índice i se tiene $\overline{X_i} \in \operatorname{Im}(h)$, luego $R(X_i;\mathbb{G}) \in K[Y_1,\ldots,Y_m]$. Como consecuencia X_i es el término líder de algún elemento de $\mathbb{G}$; como esto ocurre para cada índice i, entonces $\mathbb{G}$ contiene un elemento de la forma $X_i + G_i$ con $G_i \in K[Y_1,\ldots,Y_m]$. □

Vamos a estudiar algunos ejemplos.

Ejercicio. 20.7.
Se considera el homomorfismo $h : K[Y,Z] \longrightarrow K[X]$ definido por

$$h(Y) = X^2 - 1 \text{ y } h(Z) = X^3 - 1.$$

Calcular el núcleo y la imagen de h.

SOLUCIÓN. Siguiendo la notación de la proposición el ideal $\mathfrak{c}$ está generado por $Y - X^2 + 1$ y $Z - X^3 + 1$, ya que en este caso $\mathcal{I}(V) = 0$. Primero calculamos una base de Groebner de $\mathfrak{c}$ respecto al orden lexicográfico con $X > Y > Z$:

$$\mathbb{G} = \{3Y + 3Y^2 + Y^3 - 2Z - Z^2, -1 + X - 2Y - Y^2 + XZ, -1 + X + XY - Z, -1 + X^2 - Y\}$$

Al calcular la intersección $\mathfrak{c} \cap K[Y,Z]$, ésta está generada por:

$$\{3Y + 3Y^2 + Y^3 - 2Z - Z^2\},$$

por lo tanto h no es inyectiva, ya que el núcleo contiene a $3Y + 3Y^2 + Y^3 - 2Z - Z^2$. Para ver la sobreyectividad tenemos que ver si en $\mathbb{G}$ existe un elemento de la forma $X - G$, con $G \in K[Y,Z]$. Es claro que no, luego h no es sobreyectiva, ya que $X \notin \operatorname{Im}(h)$. □

Ejemplo. 20.8.
Se consideran

$$\begin{aligned} &V = \mathcal{V}(XZ + Y^2 + Z^2, XY - XZ - 2Z^2) \subseteq \mathbb{A}^3(\mathbb{C}) \text{ y} \\ &W = \mathcal{V}(U^3 - UV^2 + V^3) \in \mathbb{A}^2(\mathbb{C}). \end{aligned}$$

Se verifica

$$\begin{aligned} &\mathcal{I}(V) = (XZ + Y^2 + Z^2, XY - XZ - 2Z^2) \text{ y} \\ &\mathcal{I}(W) = (U^3 - UV^2 + V^3). \end{aligned}$$

¡Ya comprobaremos esto más adelante!

Se considera el homomorfismo $h : \frac{K[U,V]}{\mathcal{I}(W)} \longrightarrow \frac{K[X,Y,Z]}{\mathcal{I}(V)}$ inducido por $h' : K[U,V] \longrightarrow K[X,Y,Z]$ definido por

$$h'(U) = Z, \quad h'(V) = Y.$$

Para ver que h está bien definido basta ver que $h'(\mathcal{I}(W)) \subseteq \mathcal{I}(V)$. Observar que $h'(U^3 - UV^2 + V^3) = Z^3 - ZY^2 + Y^3$ pertenece a $\mathcal{I}(V)$, ya que una base de Groebner de $\mathcal{I}(V)$ es:

$$\{Y^3 - Y^2Z + Z^3, Y^2 + XZ + Z^2, XY + Y^2 + YZ - Z^2\}.$$

Para estudiar la inyectividad y sobreyectividad de h consideramos el ideal $\mathfrak{c}$ definido por $\{U - Z, V - Y, XZ + Y^2 + Z^2, XY - XZ + YZ - 2Z^2\}$. Una base de Groebner respecto al orden lexicográfico con $X > Y > Z > U > V$ es:

$$\mathbb{G} = \{U^3 - UV^2 + V^3, -U + Z, -V + Y, -U^2 + UV + V^2 + VX, U^2 + V^2 + UX\}.$$

Al calcular la intersección con $K[U, V]$, ésta está generada por

$$\{U^3 - UV^2 + V^3\}.$$

Observar que está contenida en $\mathcal{I}(W)$, luego h es inyectiva. Para ver si es sobreyectiva, tenemos que encontrar $X - G_1$, $Y - G_2$, $Z - G_3$ en $\mathbb{G}$, con $G_1, G_2, G_3 \in K[U, V]$. Para Y y Z es posible, pero no para X, por lo tanto $X \notin \mathrm{Im}(h)$ y h no es sobreyectiva.

Finalmente vamos a describir la aplicación polinómica que define el homomorfismo h. Tenemos que determinar F_U y F_V en $K[X, Y, Z]$ tales que $h(U) = \overline{F_U}$ y $h(V) = \overline{F_V}$; por ejemplo $F_U = Z$ y $F_V = Y$. Entonces la aplicación polinómica es:

$$f : V \longrightarrow W, \quad f(x, y, z) = (F_U(x, y, z), F_V(x, y, z)) = (z, y).$$

Aplicaciones:

Cálculo del polinomio mínimo de un elemento en una extensión algebraica simple

Proposición. 20.9.
Sea K un cuerpo y α un elemento algebraico sobre K con polinomio mínimo $F = \mathrm{Irr}(\alpha, K) \in K[X]$. Sea $\beta \in K[\alpha]$ definido por un polinomio, por ejemplo $\beta = G(\alpha)$. Si $\mathbb{G}$ es una base de Groebner reducida del ideal $(F, Y - G) \in K[X, Y]$, respecto al orden lexicográfico con $X > Y$, entonces el polinomio mínimo de β sobre K es el único polinomio en $\mathbb{G} \cap K[Y]$.

DEMOSTRACIÓN. Consideramos el siguiente diagrama:

$$\begin{array}{ccccc}
(\mathrm{Irr}(\beta, K)) & \longrightarrow & K[Y] & \longrightarrow & \frac{K[Y]}{(\mathrm{Irr}(\beta,K))} = K[\beta] \\
\downarrow & & \downarrow h' & & \downarrow h \\
(\mathrm{Irr}(\alpha, K)) & \longrightarrow & K[X] & \longrightarrow & \frac{K[X]}{(\mathrm{Irr}(\alpha,K))} = K[\alpha]
\end{array}$$

La aplicación h es la inclusión de $K(\beta)$ en $K(\alpha)$, y está definida $h(\beta) = \beta = G(\alpha)$. La aplicación h' está definida $h'(Y) = G$, entonces h' induce h si $h'(\operatorname{Irr}(\beta, K)) \subseteq (\operatorname{Irr}(\alpha, K))$, lo cual es inmediato, ya que si $H \in (\operatorname{Irr}(\beta, K))$, entonces $h'(H) = H(G)$ y se verifica: $H(G)(\alpha) = H(G(\alpha)) = H(\beta) = 0$. El núcleo de h es cero, ya que $K(\beta)$ es un cuerpo (también porque h es la inclusión). Por otro lado el núcleo es $\frac{\mathfrak{c}\cap K[Y]}{(\operatorname{Irr}(\beta,K))}$, siguiendo la notación de la Proposición (20.5.), siendo $\mathfrak{c} = (Y - G, \operatorname{Irr}(\alpha, K))$. Por lo que calculando una base de Groebner reducida $\mathbb{G}$ de $\mathfrak{c}$, un sistema de generadores de $(\operatorname{Irr}(\beta, K)) = \mathfrak{c} \cap K[Y]$ es $\mathbb{G} \cap K[Y]$. □

Ejemplo. 20.10.
Dado $K = \mathbb{Q}$ y $\alpha = \sqrt[3]{2}$, para determinar el polinomio mínimo de $\beta = 2 + \sqrt[3]{2} - \sqrt[3]{4}$, calculamos una base de Groebner de $(X^3 - 2, Y - 2 - X + X^2)$ en $\mathbb{Q}[X, Y]$ respecto al orden lexicográfico con $X > Y$. Ésta es:

$$\mathbb{G} = \{-18 + 18Y - 6Y^2 + Y^3, -6 + 3X + 3Y - Y^2\}.$$

La intersección con $K[Y]$ es:

$$\{-18 + 18Y - 6Y^2 + Y^3\},$$

y resulta que $Y^3 - 6Y^2 + 18Y - 18$ es el polinomio mínimo de β en $\mathbb{Q}$.

Es bien conocido que un elemento genérico de $K[\alpha]$ es de la forma $G(\alpha)$, para $G \in K[X]$. Sin embargo, en ciertas ocasiones podemos expresar un elemento de $K[\alpha]$ en la forma $G(\alpha)/L(\alpha)$, con $G, L \in K[X]$ y $L(\alpha) \neq 0$. Se trata de determinar el polinomio mónico irreducible de un elemento $\beta \in K[\alpha]$ expresado en la forma $\beta = G(\alpha)/L(\alpha)$.

Proposición. 20.11.
Dado $\beta = G(\alpha)/L(\alpha) \in K[\alpha]$, siendo $G, L \in K[X]$ y $F = \operatorname{Irr}(\alpha, K)$, se tiene que $\operatorname{Irr}(\beta, K)$ es el único generador de $\mathfrak{d} \cap K[Z]$, siendo $\mathfrak{d} = (F, LZ - G, LY - 1) \subseteq K[X, Y, Z]$.

DEMOSTRACIÓN. Consideramos el siguiente diagrama

$$\begin{array}{ccccc}
(\operatorname{Irr}(\beta,K)) & \longrightarrow & K[Z] & \longrightarrow & K[\beta] = \frac{K[Z]}{(\operatorname{Irr}(\beta,K))} \\
\downarrow & & \downarrow h' & & \downarrow h \\
(\operatorname{Irr}(\alpha,K), YL-1) & \longrightarrow & K[X,Y] & \stackrel{p}{\longrightarrow} & K[\alpha] = \frac{K[X,Y]}{(\operatorname{Irr}(\alpha,K),YL-1)} \\
\downarrow & & \downarrow & & \| \\
\frac{(\operatorname{Irr}(\alpha,K))+(YL-1)}{(YL-1)} & \longrightarrow & \frac{K[X,Y]}{(YL-1)} & \stackrel{q}{\longrightarrow} & K[\alpha]
\end{array}$$

Donde h es la inclusión y p está definida $p(X) = \alpha$, $p(Y) = \frac{1}{L(\alpha)}$. Entonces p se factoriza por el cociente $K[X, Y]/(YL - 1)$ a través de q. Los núcleos de p y q son sencillos de calcular. Además podemos definir $h' : K[Z] \to K[X, Y]$ mediante $h'(Z) = GY$, que hace conmutar el cuadrado superior derecha.

Como h es inyectiva, se tiene que su núcleo es cero, y por lo tanto $(\mathrm{Irr}(\beta,K)) = \mathfrak{d}\cap K[Z]$, siendo $\mathfrak{d}$ el ideal de $K[X,Y,Z]$ generado por $(Z-GY, YL-1, \mathrm{Irr}(\alpha,K)) = (LZ-G, YL-1, \mathrm{Irr}(\alpha,K))$. □

Ejemplo. 20.12.
Dado $K=\mathbb{Q}$ y $\alpha=\sqrt[3]{2}$, para determinar el polinomio mínimo de $\beta=\frac{1+\sqrt[3]{2}-\sqrt[3]{4}}{1-\sqrt[3]{2}+\sqrt[3]{4}}$, calculamos una base de Groebner de $(Z-(1+X-X^2)Y, X^3-2, Y(1-X+X^2)-1)$ en $\mathbb{Q}[X,Y,Z]$ respecto al orden lexicográfico con $X>Y>Z$. Ésta es:

$$\mathbb{G}=\{-5+3Z+9Z^2+9Z^3, -1+2Y-Z, -1+2X-3Z\}.$$

La intersección con $K[Z]$ es:

$$\{-5+3Z+9Z^2+9Z^3\},$$

y resulta que $9X^3+9X^2+3X-5$ es el polinomio mínimo de β en $\mathbb{Q}$.

Teoría de la eliminación y proyecciones

Dado un cuerpo K, para cada subconjunto $S\subseteq K^n$ tenemos que $\mathcal{VI}(S)$ es el menor subconjunto algebraico que contiene a S. En efecto, si tenemos un subconjunto algebraico W tal que $S\subseteq W\subseteq \mathcal{VI}(S)$, se tiene $\mathcal{VI}(S)\subseteq\mathcal{VI}(W)\subseteq\mathcal{VIVI}(S)=\mathcal{VI}(S)$, y por lo tanto $W=\mathcal{VI}(S)$.
Llamamos a $\mathcal{VI}(S)$ la **clausura algebraica**, o la **clausura de Zariski**, de S en K^n, y la representamos por $\overline{S}$.

Proposición. 20.13.
Consideramos $p: K^n\to K^{n-m}$ la proyección a las últimas coordenadas. Para cada conjunto algebraico $V\subseteq K^n$ con $\mathfrak{a}=\mathcal{I}(V)$ se verifica que para cada $\mathfrak{a}_m=\mathfrak{a}\cap K[X_{m+1},\dots,X_n]$, el m–ésimo ideal de eliminación de $\mathfrak{a}$, se tiene que $\mathcal{V}(\mathfrak{a}_m)$ es la clausura de Zariski de $p(V)\subseteq K^{n-m}$.

DEMOSTRACIÓN. Tenemos que $p(V)\subseteq\mathcal{V}(\mathfrak{a}_m)$, ya que para cada $F\in\mathfrak{a}_m\subseteq K[X_{n-m},X_n]$ se tiene $F(x)=0$ para cada $x\in p(V)$, y por lo tanto $\mathcal{VI}(p(V))\subseteq\mathcal{V}(\mathfrak{a}_m)$. Por otro lado, si $F\in\mathcal{I}(p(V))\subseteq K[X_{m+1},\dots,X_n]$, entonces $F(x)=0$ para cada $x\in V$, como polinomio de $K[X_1,\dots,X_n]$. Por tanto $F\in\mathcal{I}(V)=\mathfrak{a}$, y $F\in\mathfrak{a}_m$, esto es, $\mathcal{I}(p(V))\subseteq\mathfrak{a}_m$, y como consecuencia $\mathcal{V}(\mathfrak{a}_m)\subseteq\mathcal{VI}(p(V))$. □

Ejemplo. 20.14.
Consideramos el conjunto $V=\{(x,y,z)\in\mathbb{R}^3 \mid x^2+y^2-z^2=1, x+y+z=1\}$ y hacemos la proyección sobre el plano (Y,Z), esto es, el plano de ecuación $X=0$; por lo tanto si $\mathfrak{a}=(X^2+Y^2-Z^2-1)\subseteq\mathbb{R}[X,Y,Z]$, tenemos que calcular el ideal de eliminación $\mathfrak{a}\cap\mathbb{R}[Y,Z]$, que en este caso es $(-Y+Y^2-Z+YZ)=(Y-1)(Y-Z)$, que corresponde a dos rectas.
Si hacemos la proyección sobre el plano (X,Y), el plano $Z=0$, tenemos que calcular el ideal de eliminación $\mathfrak{a}\cap\mathbb{R}[X,Y]$, que en este caso es $(1-X-Y+XY)=(X-1)(Y-1)$, que corresponde a dos rectas.

Ecuaciones implícitas de un conjunto algebraico

Dado un cuerpo K y polinomios $G_1,\ldots,G_n \in K[T_1,\ldots,T_m]$, consideramos el conjunto

$$U = \{(x_1,\ldots,x_n) \in K^n \mid \text{ existe } (t_1,\ldots,t_m) \in K^m \text{ tal que } x_i = G_i(t_1,\ldots,t_m)\}.$$

Este conjunto no es necesariamente un conjunto algebraico, pero sí lo es su clausura algebraica $\overline{U} = \mathcal{VI}(U)$.

Proposición. 20.15.
En la situación anterior la clausura algebraica de U es $\mathcal{V}(\mathfrak{c}) \cap K[X_1,\ldots,X_n]$, siendo $\mathfrak{c}$ el ideal de $K[X_1,\ldots,X_n,T_1,\ldots,T_m]$ generado por $\{X_1 - G_1,\ldots,X_n - G_n\}$.

DEMOSTRACIÓN. Consideramos la aplicación polinómica $f : K^m \to K^n$ definida mediante $f(t) = (G_1(t),\ldots,G_n(t))$. El grafo W de esta aplicación es el conjunto de puntos $(t,x) \in K^m \times K^n = K^{n+m}$, y los elementos de U son los que se obtienen al proyectar a K^n. Por lo tanto la clausura algebraica de U es $\mathcal{V}(\mathfrak{a}_m)$, siendo $\mathfrak{a} = (X_1 - G_1,\ldots,X_n - G_n)$ el ideal que define a W. □

Ejemplo. 20.16.
Consideramos el conjunto de puntos $U = \{(t^2+1, t^2-1) \mid t \in \mathbb{R}\}$. Estamos interesados en determinar la clausura algebraica de U en $\mathbb{R}^2$. Para esto estudiamos el ideal

$$\mathfrak{a} = (X - T^2 - 1, Y - T^2 + 1) \subseteq \mathbb{R}[T,X,Y],$$

y eliminamos la indeterminada T; se tiene

$$\mathfrak{a} \cap \mathbb{R}[X,Y]) = (X - Y - 2).$$

Tenemos pues una recta.
Si consideramos el conjunto $U = \{(t^2+1, t-1) \mid t \in \mathbb{R}\}$, entonces las ecuaciones implícitas de la clausura algebraica son $\{X - Y^2 - 2Y - 2\}$; se trata de una parábola.

Un caso más general es aquel en el que U no está definido por polinomios, sino por funciones racionales $G_1/H_1,\ldots,G_n/H_n$, en donde $G_1,\ldots,G_n,H_1,\ldots,H_n \in K[X_1,\ldots,X_n]$. Tenemos

$$U = \{(x_1,\ldots,x_n) \in K^n \mid \text{ existe } (t_1,\ldots,t_m) \in K^m \text{ tal que } x_i = G_i(t_1,\ldots,t_m)/H_i(t_1,\ldots,t_m)\}.$$

Consideramos la siguiente composición:

$$K[X_1,\ldots,X_n] \longrightarrow K[T_1,\ldots,T_m,S_1,\ldots,S_n] \longrightarrow K[T_1,\ldots,T_m,S_1,\ldots,S_n]/(S_1H_1 - 1,\ldots,S_nH_n - 1)$$

Es una aplicación polinómica, y podemos calcular su núcleo; éste es:

$$(S_1H_1 - 1,\ldots,S_nH_n - 1, X_1 - G_1S_1,\ldots,X_n - G_nS_n) \cap K[X_1,\ldots,X_n].$$

Este homomorfismo define una aplicación polinómica $\mathcal{V}(S_1H_1-1,\dots,S_nH_n-1)\to K^n$, y su grafo es (t,x), siendo $S_i(t)H_i(t)=1$ y $x=(G_i(t)S_i(t))_i$. Como consecuencia la proyección en la segunda componente es exactamente el conjunto U, y su clausura algebraica es $\mathcal{V}((S_1H_1-1,\dots,S_nH_n-1,X_1-G_1S_1,\dots,X_n-G_nS_n)\cap K[X_1,\dots,X_n])$.

Proposición. 20.17.
En la situación anterior la clausura algebraica de U es $\mathcal{V}(\mathfrak{c}\cap K[X_1,\dots,X_n])$, siendo $\mathfrak{c}$ el ideal de $K[X_1,\dots,X_n,S_1,\dots,S_n,T_1,\dots,T_m]$ generado por $\{S_1H_1-1,\dots,S_nH_n-1,X_1-G_1S_1,\dots,X_n-G_nS_n\}$.

Ejemplo. 20.18.
Consideramos el conjunto de puntos $U=\{((t^2+1)/(t-1),(t^2-1)/t)\mid t\in\mathbb{R}\setminus\{0,1\}\}$. Estamos interesados en determinar la clausura algebraica de U en $\mathbb{R}^2$. Para esto estudiamos el ideal

$$\mathfrak{a}=((T-1)X-T^2-1,TY-T^2+1)\subseteq\mathbb{R}[T,X,Y],$$

y eliminamos la indeterminada T; se tiene

$$\mathfrak{a}\cap\mathbb{R}[X,Y])=(X^2Y-XY^2-4X-Y^2-4).$$

Si consideramos el conjunto $U=\{((t^2+1)/t,(t-1)/t)\mid t\in\mathbb{R}\}$, entonces las ecuaciones implícitas de la clausura algebraica son $\{XY-X-Y^2+2Y-2\}$.

Ejemplo. 20.19.
Consideramos el conjunto $U=\{(cos(t),sen(t))\mid t\in\mathbb{R}\}$. Para determinar la clausura algebraica de U consideramos el ideal $\mathfrak{a}=(X-cos(t),Y-sen(t))\subseteq K[X,Y]$. Tenemos dos funciones *sen* y *cos* que verifican propiedades adicionales. Si llamamos $L=sen(t)$ y $M=cos(t)$, se tiene la relación $L^2+M^2=1$. Podemos entonces trabajar en el anillo $\mathbb{R}[X,Y,L,M]$ con el ideal $\mathfrak{b}=(X-M,Y-L,L^2+M^2-1)$. Para obtener las ecuaciones implícitas necesitamos eliminar las variables L y M, esto es, determinar el ideal $\mathfrak{b}\cap\mathbb{R}[X,Y]=(X^2+Y^2-1)$.

Ejemplo. 20.20.
Consideramos el conjunto $U=\{(cos(t),sen(2t))\mid t\in\mathbb{R}\}$. Para determinar la clausura algebraica de U, llamamos $L=sen(t)$ y $M=cos(t)$; tenemos la relación $L^2+M^2=1$. Además $sen(2t)=2sen(t)cos(t)$, luego consideramos el ideal $\mathfrak{a}=(X-cos(t),Y-sen(2t),sen^2(t)+cos^2(t)-1,sen(2t)=2sen(t)cos(t))\subseteq K[X,Y]$. Utilizando L y M resulta el ideal $\mathfrak{b}=(X-M,Y-2LM,L^2+M^2-1)\subseteq\mathbb{R}[X,Y,L,M]$. Para obtener las ecuaciones implícitas necesitamos eliminar las variables L y M, esto es, determinar el ideal $\mathfrak{b}\cap\mathbb{R}[X,Y]=(4X^4-4X^2+Y^2)$.

Multiplicadores de Lagrange

Sea $A\subseteq\mathbb{R}^n$ un abierto. Dada una familia de funciones $g_i:A\to\mathbb{R}$, $i=1,\dots,t$, podemos definir un conjunto $V=\{x\in A\mid g_i(x)=0,\ \text{para todo}\ i=1,\dots,t\}$. Si $f:A\subseteq\mathbb{R}^n\longrightarrow\mathbb{R}$ es una función, un

extremo relativo de f sujeto a las condiciones $g_i(x) = 0$ es un extremo relativo de $f_{|V}$. La función f se llama la función de costo, y las funciones g_i se llaman las restricciones.

El **Teorema de los multiplicadores de Lagrange** afirma que, en estas condiciones, *si las funciones $f, g_1, \ldots, g_t$ son continuamente derivables con $t < n$, y $x \in V$ es un extremo relativo, existen $\lambda_0, \lambda_1, \ldots, \lambda_t \in \mathbb{R}$, no todos nulos, tales que*

$$\lambda_0 \nabla f(x) = \sum_{i=1}^{t} \lambda_i \nabla g_i(x).$$

Observa que si los $\{\nabla g_i(x) \mid i = 1, \ldots, t\}$ son linealmente independientes, podemos tomar $\lambda_0 = 1$.

Aplicado este resultado, podemos fácilmente determinar máximos y mínimos relativos de una función polinómica sujeta a restricciones.

Ejemplo. 20.21.
Considera la función $f(x, y, z) = x^2y^2 + 2xz - y^2z - 2z^2$ y determina los máximos y mínimos relativos sujetos a las condiciones: $g_1(x, y, z) := x^2 - y^2 - z^2 + 1 = 0$ y $g_2(x, y, z) := x^2 + y^2 + z^2 - 25 = 0$.

Primero determinamos los vectores gradientes ∇f, ∇g_1 y ∇g_2:

$$\begin{aligned}
&\nabla f = (2xy^2, 2x^2y - 2yz, -y^2 - 4z),\\
&\nabla g_1 = (2x, -2y, -2z),\\
&\nabla g_2 = (2(-1 + x), 2y, 2z).
\end{aligned}$$

A continuación establecemos la ecuación con los multiplicadores de Lagrange:

$$\nabla f = \lambda_1 \nabla g_1 + \lambda_2 \nabla g_2$$

En nuestro ejemplo se tiene:

$$\begin{aligned}
2xy^2 + 2z &= \ \ 2\lambda_1 x + 2\lambda_2(-1 + x)\\
2x^2y - 2yz &= -2\lambda_1 y + \qquad 2\lambda_2 y\\
2x - y^2 - 4z &= -2\lambda_1 z + \qquad 2\lambda_2 z
\end{aligned}$$

Los posible puntos críticos verifican las ecuaciones:

$$\begin{aligned}
&x^2 - y^2 - z^2 + 1 = 0\\
&x^2 + y^2 + z^2 - 25 = 0\\
&2xy^2 + 2z - 2\lambda_1 x - 2\lambda_2(-1 + x) = 0\\
&2x^2y - 2yz + 2\lambda_1 y - 2\lambda_2 y = 0\\
&2x - y^2 - 4z + 2\lambda_1 z - 2\lambda_2 z = 0
\end{aligned}$$

Basta pues con eliminar λ_1 y λ_2 para obtener los puntos críticos. En este caso tenemos que resolver una

sistema con cuatro ecuaciones:

$$\left.\begin{array}{c}332741+1809004z+1618124z^2-721792z^3-251880z^4+81392z^5+6896z^6-2688z^7\\ +144z^8=0\\ \\ 529y+2876yz+2660yz^2-672yz^3+36yz^4=0\\ \\ -100791548115+5110113382y^2-63413291047z+34559085744z^2+9491000668z^3\\ -3599594844z^4-238936268z^5+113793504z^6-6320304z^7=0\\ \\ -36915130840+5110113382x-63413291047z+29448972362z^2+9491000668z^3\\ -3599594844z^4-238936268z^5+113793504z^6-6320304z^7=0\end{array}\right\}$$

Ejemplo. 20.22.
Si consideramos ahora las funciones $f(x,y,z) = x^2y^2+2x^4+2$ con las restricciones: $g_1(x,y,z) := x^2-y^2-z^2+1 = 0$ y $g_2(x,y,z) := x^2+y^2+z^2-25 = 0$; tras plantear las ecuaciones de los multiplicadores de Lagrange se tiene que los puntos críticos son las ocho soluciones del sistema:

$$\left.\begin{array}{r}629z-104z^3+4z^5=0\\ yz=0\\ 629-104y^2+4y^4-104z^2+4z^4=0\\ 25+2x-2y^2-2z^2=0\end{array}\right\}$$

21. Ejercicios

Funciones polinómicas

Ejercicio. 21.1. (AM, Cap 1, Ej 27)
Sea V un conjunto algebraico, para cada $x \in X$ se considera $\mathfrak{m}_x = \{f \in K[V] \mid f(x) = 0\}$. Se tiene:
(1) $\mathfrak{m}_x$ es un ideal maximal de $K[V]$.
(2) La aplicación $\lambda : V \longrightarrow \mathrm{Max}(K[V])$, $\lambda(x) = \mathfrak{m}_x$, es una aplicación inyectiva.
(3) La aplicación λ es una aplicación sobreyectiva si K es algebraicamente cerrado.

SOLUCIÓN

Ejercicio. 21.2.
Sea $V \subseteq \mathbb{A}^n(K)$ un conjunto algebraico afín finito de cardinal m. Demuestra que $K[V] \cong K^m$ como K-álgebras.
(Pista: Utiliza el teorema chino del resto.)

SOLUCIÓN

Anillos de funciones

Ejercicio. 21.3.
Se considera $A = \mathcal{C}(\mathbb{R})$ el conjunto de las aplicaciones continuas $f : \mathbb{R} \to \mathbb{R}$. En A se definen dos operaciones:

$$(f+g)(x) = f(x) + g(x), \ \text{y}$$
$$(f \cdot g)(x) = f(x)g(x).$$

Para cada $x \in \mathbb{R}$.
(1) Prueba que $(A, +, \cdot, 1)$ es un anillo conmutativo que no es un dominio de integridad.

Para cada $r_0 \in \mathbb{R}$ se define $\mathfrak{a}_{r_0} = \{f \in A \mid f(r_0) = 0\}$.
(2) Prueba que $\mathfrak{a}_{r_0}$ es un ideal para cada $r_0 \in \mathbb{R}$.

SOLUCIÓN

Ejercicio. 21.4.
Consideramos $A = \mathcal{A}([0,1], \mathbb{R})$ el conjunto de las aplicaciones de $[0,1]$ a $\mathbb{R}$ con operaciones definidas punto a punto.

(1) Prueba que A es un anillo que no es un dominio de integridad.
(2) Determina los elementos regulares de A.

SOLUCIÓN

Ejercicio. 21.5.
Se define $B = \mathcal{C}([0,1],\mathbb{R})$ el conjunto de las aplicaciones continuas de $[0,1]$ a $\mathbb{R}$.

(3) Prueba que B es un subanillo de A.

Para cada elemento $r_0 \in [0,1]$ se define $\mathfrak{m}_{r_0} = \{f \in B \mid f(r_0) = 0\}$.

(4) Prueba que cada $\mathfrak{m}_{r_0}$ es un ideal maximal de B.
(5) Prueba que para cada ideal maximal $\mathfrak{m}$ de B existe un elemento $r \in [0,1]$ tal que $\mathfrak{m} = \mathfrak{m}_{r_0}$.
(6) Prueba que en el caso de $B = \mathcal{C}(\mathbb{R},\mathbb{R})$ no todos los ideales maximales de B son de la forma $\mathfrak{m}_r$ para algún $r \in \mathbb{R}$.

SOLUCIÓN

Ejercicio. 21.6.
Sea X un espacio topológico y $\mathcal{C}(X) = \{f : X \to \mathbb{R} \mid f \text{ es continua}\}$. Llamamos $Z(f) = \{x \in X \mid f(x) = 0\}$, es un cerrado de X.

(1) $Z(f) \cup Z(g) = Z(fg)$.
(2) $Z(f) \cap Z(g) = Z(f^2 + g^2)$.
(3) $(f,g) = \mathcal{C}(X)$ si, y sólo si, $Z(f) \cap Z(g) = \varnothing$.
(4) Si $\mathfrak{p},\mathfrak{q}$ son ideals primos de $\mathcal{C}(X)$, entonces $\mathfrak{p}\mathfrak{q} = \mathfrak{p} \cap \mathfrak{q}$.
(5) En particular para cada ideal primo $\mathfrak{p}$ de $\mathcal{C}(X)$ se tiene $\mathfrak{p}^2 = \mathfrak{p}$.

SOLUCIÓN

Conjuntos algebraicos

Ejercicio. 21.7.
Estudia los siguientes enunciados:
(1) Para cada $F \in K[X]$ no constante, describe $\mathcal{V}(F) \subseteq \mathbb{A}^1(K)$ en términos de la factorización de F en $K[X]$.
(2) Usa dicha descripción para determinar $\mathcal{I}(\mathcal{V}(F))$.
(3) Deduce que $\mathcal{I}(\mathcal{V}(F)) = (F)$ si y sólo si F es el producto en $K[X]$ de factores irreducibles distintos.

SOLUCIÓN

Ejercicio. 21.8.
Sean F, $G \in K[X,Y]$ polinomios irreducibles no asociados. Demuestra que $\mathcal{V}((F,G)) \subseteq \mathbb{A}^2(K)$ es vacío o un conjunto finito.
(Pista: Si $(F,G) \neq (1)$, demuestra que (F,G) contiene un polinomio no nulo de $K[X]$ tomando F, $G \in K(X)[Y]$ y aplicando el lema de Gauss para demostrar que F y G son primos relativos en $K(X)[Y]$.)

SOLUCIÓN

Ejercicio. 21.9.
Estudia los siguientes enunciados:

(1) Identificamos cada matriz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(K)$ con el punto $(a,b,c,d) \in \mathbb{A}^4(K)$. Demuestra que el grupo $SL_2(K)$ de la matrices determinante igual a 1 es un conjunto algebraico de $\mathbb{A}^4(K)$.
(2) Demuestra que $SL_n(K)$ es un conjunto algebraico de $\mathbb{A}^{n^2}(K)$.

SOLUCIÓN

Ejercicio. 21.10.
Sea V cualquier recta de $\mathbb{R}^2$. Demuestra que $\mathbb{R}[V] \cong \mathbb{R}[Z]$, Z es una indeterminada sobre $\mathbb{R}$, como $\mathbb{R}$–álgebras. Describe el isomorfismo de conjuntos algebraicos correspondiente de $\mathbb{A}^1(\mathbb{R})$ a V.

SOLUCIÓN

Ejercicio. 21.11.
Un conjunto algebraico V es irreducible si, y solo si, $\mathcal{I}(V)$ es un ideal primo.

SOLUCIÓN

Ejercicio. 21.12.
Trabajamos sobre $\mathbb{C}$.

(1) Sea $V = \mathcal{V}(X^3YZ - 5X^4Y + 7XZ)$. Prueba que $\mathcal{I}(V) = (X^3YZ - 5X^4Y + 7XZ)$.
(2) Sea $V = \mathcal{V}(X^2 + Y^2 - 2Z^2 - XZ)$. Prueba que $\mathcal{I}(V) = (X^2 + Y^2 - 2Z^2 - XZ)$.

SOLUCIÓN

Ejercicio. 21.13.
Sean K un cuerpo y $a_1,\dots,a_n \in K$ elementos de K. Prueba que el conjunto $\mathfrak{m} = \{F \in K[X_1,\dots,X_n] \mid F(a_1,\dots,a_n) = 0\}$ es el ideal maximal de $K[X_1,\dots,X_n]$ generado por $X_1 - a_1,\dots,X_n - a_n$.

SOLUCIÓN

Anillos coordenados

Ejercicio. 21.14.
Sea $V = \mathcal{V}(XY - Z) \in \mathbb{A}^3(\mathbb{R})$. Demuestra que V es isomorfa a $\mathbb{A}^2(\mathbb{R})$ y describe explícitamente un isomorfismo f y el correspondiente isomorfismo de $\mathbb{R}$–álgebras $\widetilde{f} : K[V] \longrightarrow K[\mathbb{A}^2(\mathbb{R})]$. Describe los isomorfismos inversos.
¿Es $W = \mathcal{V}(XY - Z^2)$ isomorfo a $\mathbb{A}^2(\mathbb{R})$?

SOLUCIÓN

Ejercicio. 21.15.
Sea $V = \mathcal{V}(XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subseteq \mathbb{A}^3(K)$, con $K = \mathbb{R}$.

(1) Demuestra que la aplicación $f : \mathbb{A}^1(K) \longrightarrow V$, definida por $f(t) = (t^3, t^4, t^5)$ es una aplicación sobreyectiva.
(2) Describe explícitamente el correspondiente homomorfismo de K-álgebras $\widetilde{f} : K[V] \longrightarrow K[\mathbb{A}^1]$.
(3) Demuestra que $\widetilde{f}$ no es un isomorfismo.

SOLUCIÓN

Ejercicio. 21.16.
Sea $V = \mathcal{V}(Y^4 - X^5) \subseteq \mathbb{A}^2(K)$, con $K = \mathbb{C}$.

(1) Demuestra que la aplicación $f : \mathbb{A}^1(K) \longrightarrow V$, definida por $f(t) = (t^4, t^5)$ es una aplicación biyectiva.
(2) Describe explícitamente el correspondiente homomorfismo de K-álgebras $\widetilde{f} : K[V] \longrightarrow K[\mathbb{A}^1]$.
(3) Demuestra que $\widetilde{f}$ no es un isomorfismo.

SOLUCIÓN

Ejercicio. 21.17.
Sea $\mathbb{G} = \{G_1, \ldots, G_m\}$ una base de Groebner del ideal $\mathfrak{a}$ del anillo $K[X_1, \ldots, X_n]$. Sea $\mathbb{B}$ el conjunto de monomios M de $K[X_1, \ldots, X_n]$ que no son divisibles por ninguno de los $\operatorname{lt}(G_i)$, $i = 1, \ldots, m$. Demuestra que $\mathbb{B}$ es una base del cociente $K[X_1, \ldots, X_n]/\mathfrak{a}$ como espacio vectorial sobre K.

SOLUCIÓN

Ejercicio. 21.18.
Sea $\mathfrak{a} = (X^3Y - XY^2 + 1, X^2Y^2 - Y^3 - 1) \subseteq K[X, Y]$, con $K = \mathbb{Q}$.

(1) Utiliza el ejercicio previo para demostrar que $\mathbb{B} = \{1, Y, Y^2, Y^3\}$ es una base del K-espacio vectorial $K[X, Y]/\mathfrak{a}$
(2) Calcula la tabla de multiplicación para los elementos de $\mathbb{B}$.

SOLUCIÓN

Ejercicio. 21.19.
Sean $V = \mathcal{V}(X^3 - X^2Z - Y^2Z)$, $W = \mathcal{V}(X^2 + Y^2 - Z^2)$ dos conjuntos algebraicos de $\mathbb{C}^3$. Entonces $\mathcal{I}(V) = (X^3 - X^2Z - Y^2Z)$, $\mathcal{I}(W) = (X^2 + Y^2 - Z^2)$. Demuestra que $f(a, b, c) = (a^2c - b^2c, 2abc, -a^3)$ define un morfismo de V a W.

SOLUCIÓN

Ejercicio. 21.20.
Sea $V = \mathcal{V}(X^3 + Y^3 + 7Z^3) \subseteq \mathbb{C}^3$. Entonces $\mathcal{I}(V) = (X^3 + Y^3 + 7Z^3) \subseteq \mathbb{C}[X, Y, Z]$.

(1) Demuestra que $\widetilde{f}(X) = X(Y^3 - 7Z^3)$, $\widetilde{f}(Y) = Y(7Z^3 - X^3)$, $\widetilde{f}(Z) = Z(X^3 - Y^3)$ define un homomorfismo de $\mathbb{C}$-álgebras de $\mathbb{C}[V]$ consigo mismo.
(2) Sea $f : V \longrightarrow V$ el morfismo correspondiente a $\widetilde{f}$. Comprueba que $(-2, 1, 1) \in V$ y calcula $f(-2, 1, 1) \in V$.
(3) Demuestra que existen infinitos puntos $(a, b, c) \in V$ tales que $a, b, c \in \mathbb{Z}$ y $\operatorname{m.c.d.}\{a, b, c\} = 1$.

SOLUCIÓN

Ejercicio. 21.21.
Sean $V = \mathcal{V}(XZ + Y^2 + Z^2, XY - XZ + YZ - 2Z^2) \subseteq \mathbb{C}^3$ y $W = \mathcal{V}(U^3 - UV^2 + V^3) \subseteq \mathbb{C}^2$.

(1) Demuestra que la aplicación $f(a,b) = (-2a^2+ab, ab-b^2, a^2-ab)$ define un morfismo $W \longrightarrow V$.
(2) Demuestra que el núcleo del homomorfismo de $\mathbb{C}$-álgebras correspondiente $\mathbb{C}[V] \longrightarrow \mathbb{C}[W]$ es el ideal (X^2+3Y^2+YZ).

SOLUCIÓN

Ejercicio. 21.22.
Definimos $h : \mathbb{Q}[U,V,W] \longrightarrow \mathbb{Q}[X,Y]$ mediante $h(U) = X^2+Y$, $h(V) = X+Y^2$, $h(W) = X-Y$.

(1) Demostrar que ni X ni Y están en la imagen de h.
(2) Demostrar que $F = 2X^3-4XY-2Y^3-4Y$ está en la imagen de h y determinar un polinomio $G \in \mathbb{Q}[U,V,W]$ tal que $h(G) = F$.
(3) Demostrar que $\operatorname{Ker}(h) = (U^2-2UV-2UW^2+4UW+V^2-2VW^2-4VW+W^4+3W^3)$.

SOLUCIÓN

Ejercicio. 21.23.
Sea α una raíz del polinomio irreducible $F(X) \in K[X]$ y sea $\beta = G(\alpha)/L(\alpha)$, donde $G, L \in K[X]$ y $L(\alpha) \neq 0$.

(1) Razonar que existen polinomios $S, T \in K[X]$ tales que $SL+TF = 1$ y razonar que $\beta = H(\alpha)$, donde $H = GS$.
(2) Demostrar que los ideales $(F, Y-H)$ y $(F, LY-G)$ de $K[X,Y]$ son iguales.
(3) Deducir que el polinomio mínimo para β es el polinomio mónico en $\mathbb{G} \cap K[Y]$, donde $\mathbb{G}$ es la base de Groebner reducida del ideal $(F, LY-G) \subseteq K[X,Y]$ para el orden lexicográfico con $X > Y$.
(4) Halla el polinomio mínimo sobre $\mathbb{Q}$ de $\beta = \dfrac{3-\sqrt[3]{2}+\sqrt[3]{4}}{1+3\sqrt[3]{2}-3\sqrt[3]{4}}$.

SOLUCIÓN

Ejercicio. 21.24.
Se consideran V y W los conjuntos algebraicos definidos por $V = \{(t^2,t^3,t^4) \mid t \in \mathbb{R}\}$ y $W = \{(t^2,t^4,t^5) \mid t \in \mathbb{R}\}$.

(1) Comprueba que la aplicación $f : V \longrightarrow W$ definida $f(a,b,c) = (a,c,ab)$ es una aplicación polinómica de V a W.
(2) Si $\mathcal{I}(V) = (X_1^3-X_2^2, X_1^2-X_3)$ y $\mathcal{I}(W) = (X_1^2-X_2, X_1^5-X_3^2)$, calcula el homomorfismo $\widetilde{f} : K[W] \longrightarrow K[V]$.

(3) Calcula el núcleo de $\widetilde{f}$.
(4) Calcula la imagen de $\widetilde{f}$.

SOLUCIÓN

Ejercicio. 21.25.
Sea $K = \mathbb{C}$.Se considera el homomorfismo $f : K[X,Y,Z] \to K[X,Y]$ definido por $f(X) = X^2 + Y$, $f(Y) = X + Y^2, f(Z) = X^2 + Y^2$. Este homomorfismo determina una aplicación de $\mathbb{A}^2(K)$ a $\mathbb{A}^3(K)$.

(1) Determina el núcleo del homomorfismo f.
(2) ¿Es la aplicación de $\mathbb{A}^2(K)$ a $\mathbb{A}^3(K)$ biyectiva?
(3) ¿Cuál es la imagen de la recta V de ecuación $Y = X - 1$? Determina el ideal $\mathcal{I}(f(V))$.
(4) Haz el mismo proceso para la curva C de ecuación $Y = X^2 + 1$.

SOLUCIÓN

Aplicaciones

Ejercicio. 21.26.
Se considera el conjunto algebraico $V(X^2 + Y^2 + Z^2 - 1)$ y llamamos W_i a la intersección con el plano $V_1 = V(X + 2Y - Z)$, y $V_2 = V(X - Y - 2Z)$. Establece una biyección entre W_i y la circunferencia $V(X^2 + Y^2 - 1, Z)$.

SOLUCIÓN

Ejercicio. 21.27.
Se considera $K = \mathbb{C}$, el conjunto algebraico $V = \{(1,2),(1,3),(1,4)\}$, el conjunto algebraico $W = \mathcal{V}((Y_1 - 1)^2)$ y la aplicación $f : V \longrightarrow W$ definida $f(1,2) = (1,4,3), f(1,3) = (1,9,4)$ y $f(1,4) = (1,16,5)$.

(1) Calcula el homomorfismo $\widetilde{f} : K[W] \longrightarrow K[V]$.
(2) Calcular el núcleo de $\widetilde{f}$.
(3) Calcula la imagen de $\widetilde{f}$.
(4) Se considera la aplicación $g : K[V] \longrightarrow K[W]$, definida por $g(X_1) = Y_1$, $g(X_2) = Y_3 - Y_1$. ¿Está g bien definida?
(5) De forma natural $K[W]$ es isomorfo a $K[Y_2, Y_3]$ y $K[V]$ es isomorfo a $K \times K \times K$. Describe estos isomorfismos y da una descripción explícita del homomorfismo que induce $\widetilde{f}$ de $K[Y_2, Y_3]$ a $K \times K \times K$.

SOLUCIÓN

Ejercicio. 21.28.
Determina el polinomio mínimo de $\beta = \dfrac{1-\sqrt[4]{5}}{1+\sqrt[4]{5}+2\sqrt{5}}$ *sobre* $\mathbb{Q}$.

SOLUCIÓN

Ejercicio. 21.29.
Determina el polinomio mínimo de $\frac{\sqrt[3]{2}-1}{\sqrt[3]{4}-1}$ *sobre* $\mathbb{Q}$.

SOLUCIÓN

Ejercicio. 21.30.
Una forma de representar gráficamente en Mathematica la curva $X^3 - Y^2$ *es mediante la orden*

ContourPlot[X^3 *-* Y^2 *== 0, {X, -1, 1}, {Y, -1, 1}]*

Representa las siguientes curvas en los intervalos que se indican:

$$\begin{array}{ll} X^2Y+0{,}1Y-X, & -5<X<5,-5<Y<5 \\ (X-1)^2(X^2+Y^2)-X^2, & -3<X<3,-3<Y<3 \\ X^4-(X^2-Y^2), & -3<X<3,-3<Y<3 \\ X^2+Y^2-2, & -3<X<3,-3<Y<3 \\ X^2/9+Y^2/4-1, & -3<X<3,-3<Y<3 \\ X^2-Y^2-1, & -3<X<3,-3<Y<3 \\ XY-1, & -3<X<3,-3<Y<3 \\ X(X^2-2X+2)-2Y^2, & -1<X<5,-2<Y<2 \\ X(X^2-2X+1)-2Y^2, & -1<X<5,-2<Y<2 \\ X(X^2-2X-1)-Y^2, & -1<X<5,-2<Y<2 \end{array}$$

SOLUCIÓN

Ejercicio. 21.31.
Considerar tres parejas de estas curvas y estudiar si son o no isomorfas.

SOLUCIÓN

Ejercicio. 21.32.
Se considera $\alpha = \dfrac{1+\sqrt{2}}{1+\sqrt{2}i}$*; queremos saber si la extensión* $\mathbb{Z} \subseteq \mathbb{Z}[\alpha]$ *es entera. Para ello, determina el polinomio mínimo sobre* $\mathbb{Q}$ *de* α*. ¿Es entera esta extensión?*

SOLUCIÓN

Ejercicio. 21.33.
Dado un conjunto C *del espacio afín* $\mathbb{A}^n(K)$ *definido por las ecuaciones:*

$$\begin{cases} X_1 = F_1(T_1,\ldots,T_s) \\ \quad\vdots \\ X_n = F_n(T_1,\ldots,T_s) \end{cases}$$

donde $F_1,\ldots,F_n \in K[T_1,\ldots,T_s]$ *son polinomios, por eliminación, con el orden lexicográfico para* $T_1 > \cdots > T_s > X_1 > \cdots > X_n$*, tenemos un conjunto de polinomios* $G_1,\ldots,G_t \in K[X_1,\ldots,X_n]$*. Se verifica que* $C \subseteq V(G_1,\ldots,G_t)$*, y en general no se va a tener la igualdad. Este proceso se llama de* implicitación o de eliminación de parámetros.
Como aplicación dar ecuaciones implícitas para los siguientes conjuntos definidos dados por ecuaciones paramétricas.
(1) $X = T^2, \quad Y = T^3, \quad Z = T^4.$
(2) $X = S^2 + T, \quad Y = S + T^2, \quad Z = T + 2.$
(3) $X = S + T^2, \quad Y = S - 2T^2, \quad Z = T.$

SOLUCIÓN

Ejercicio. 21.34.
Encuentra ecuaciones implícitas para los siguientes conjuntos dados por ecuaciones paramétricas:
(1) $\{(x,y,z) \mid x = t\cos(s),\ y = t\sin(s),\ z = t^2+1\}.$
(2) $\{(x,y,z) \mid x = t(2\cos(s)+\cos(2s)),\ y = t(2\sin(s)-\sin(2s)),\ z = t\}.$

y comprueba que cada punto de estos conjuntos cumple con las ecuaciones obtenidas.

SOLUCIÓN

Capítulo IV

Módulos

Introducción

En el estudio moderno de los anillos y las álgebras las representaciones son una herramienta fundamental. La teoría general de representaciones se realiza a través del concepto de módulo, del que aquí vamos a dar su definición y sus propiedades elementales.

Haremos uso de las construcciones del módulo cociente y de la suma directa para construir módulos libres y probar que todo módulo es un cociente de un módulo libre. A continuación nos centramos en el estudio de los módulos finitamente generados y de los anillos y módulos noetherianos, en los que se encuadran la mayor parte de los ejemplos que vamos a estudiar en este curso.

22. Módulos

Definición de módulo

En este capítulo A va a ser siempre un anillo conmutativo. Un A-**módulo** es un grupo abeliano M junto con un homomorfismo de anillos $\beta : A \longrightarrow \operatorname{End}(M)$.

Para cada $a \in A$ y $m \in M$, el elemento $\beta(a)(m)$ lo representamos por am.

Para cualesquiera $a, a_1, a_2 \in A$ y $m, m_1, m_2 \in M$ se verifican las siguientes propiedades:

(M-I) $a(m_1 + m_2) = am_1 + am_2$.
(M-II) $(a_1 + a_2)m = a_1m + a_2m$.
(M-III) $a_1(a_2m) = (a_1a_2)m$.
(M-IV) $1m = m$.

Estas cuatro propiedades caracterizan también a los A-módulos en el siguiente sentido: *es equivalente que M sea un A-módulo con homomorfismo $\beta : A \longrightarrow \operatorname{End}(M)$ y que exista una aplicación $\alpha : A \times M \longrightarrow M$ verificando las propiedades (M–i) a (M–iv) anteriores.*

La aplicación α se llama una **acción** de A sobre M y β se llama el **homomorfismo de la acción**. Es claro que α y β están relacionados por la siguiente fórmula:

$$\alpha(a, m) = \beta(a)(m) \text{ para cualesquiera } a \in A \text{ y } m \in M.$$

Cambio de anillo

Sean A y B anillos conmutativos, $f : B \longrightarrow A$ un homomorfismo de anillos y M un A-módulo con homomorfismo $\beta : A \longrightarrow \operatorname{End}(M)$, entonces M también es un B-módulo con estructura dada por la composición $\beta \circ f : B \longrightarrow \operatorname{End}(M)$.

Aritmética de módulos

Los siguientes resultados señalan las propiedades básicas de la acción de un anillo sobre un módulo.

Lema. 22.1.
Sea M un A–módulo, para cada $a \in A$ y cada $m \in M$ se verifica:
(1) $a0 = 0$.
(2) $a(-m) = -(am)$.
(3) $0m = 0$.
(4) $(-a)m = -(am)$.

Lema. 22.2.
Sea M un A–módulo, para cualesquiera a, $a_i \in A$, $i \in I$ (finito) y m, $m_j \in M$, $j \in J$ (finito), se verifica:
(1) $a(\sum_{j\in J} m_j) = \sum_{j\in J} am_j$.
(2) $(\sum_{i\in I} a_i)m = \sum_{i\in I} a_i m$.

23. Homomorfismos de A–módulos

Sean A un anillo y M y M' dos A-módulos. Una aplicación $f : M \longrightarrow M'$ se llama un **homomorfismo de A–módulos** si verifica:

(HM-I) f es un homomorfismo de grupos abelianos.
(HM-II) $f(am) = af(m)$, para todo $a \in A$ y $m \in M$.

Esto es, el siguiente diagrama es conmutativo.

$$\begin{array}{ccc} A \times M & \xrightarrow{\alpha_M} & M \\ {\scriptstyle A\times f}\downarrow & & \downarrow{\scriptstyle f} \\ A \times M' & \xrightarrow{\alpha_{M'}} & M' \end{array}$$

Lema. 23.1.
Sean A un anillo, M y M' dos A-módulos y $f : M \longrightarrow M'$ una aplicación, son equivalentes:
(a) f es un homomorfismo de A-módulos.
(b) Para cualesquiera $a_1, a_2 \in A$ y $m_1, m_2 \in M$ se tiene: $f(a_1m_1 + a_2m_2) = a_1f(m_1) + a_2f(m_2)$.

Lema. 23.2.
(1) Para cada A–módulo M la identidad, id_M, es un homomorfismo de A-módulos.
(2) La composición de homomorfismos de A-módulos, cuando está definida, es un homomorfismo de A-módulos.

Submódulos

Sean A un anillo y M un A-módulo. Un subgrupo abeliano N de M se llama un **submódulo** si para cada $a \in A$ y cada $n \in N$ se tiene $an \in N$.

Lema. 23.3.
Sean A un anillo, M un A-módulo y N un subconjunto no vacío de M, son equivalentes:
(a) N es un submódulo de M;
(b) Para todos $a_1, a_2 \in A$ y $n_1, n_2 \in N$ se tiene $a_1n_1 + a_2n_2 \in N$.

Si N es un submódulo de M, entonces la inclusión $i : N \longrightarrow M$ es un homomorfismo de A-módulos.

En el conjunto $\mathcal{L}(M)$, de los submódulos de un A-módulo M, definimos la relación $\leq$ mediante:

$$N_1 \leq N_2 \text{ si } N_1 \subseteq N_2.$$

Lema. 23.4.
La relación $\leq$ es una relación de orden en $\mathcal{L}(M)$.

Proposición. 23.5.
Sean A un anillo y M un A-módulo. Para cada familia de submódulos de M, por ejemplo $\{N_i \mid i \in I\}$, se tiene que $\cap\{N_i \mid i \in I\}$ es también un submódulo de M.
Se tiene entonces que $\cap_i N_i$ es el ***ínfimo*** *de la familia $\{N_i \mid i \in I\}$.*

Como consecuencia tenemos que cada familia de submódulos tiene ínfimo. Veamos dos aplicaciones de este hecho.

Corolario. 23.6.
Sea X un subconjunto de un A-módulo M, existe un menor submódulo, AX, de M que contiene a X, y que se puede describir como

$$AX = \cap\{N \mid N \text{ es un submódulo de } M \text{ que contiene a } X\}.$$

El submódulo AX se llama el submódulo de M **generado** por X, y diremos que X es un **sistema de generadores** de AX. Cuando $X = \{x\}$, tiene un sólo elemento, $Ax := AX$ se llama el **submódulo cíclico** generado por x. Si X es un conjunto finito, entonces AX se llama un **submódulo finitamente generado**.

Podemos observar que si X es un subconjunto de un A–módulo M, el submódulo de AX generado por X consta de los siguientes elementos:

$$\{a_1x_1 + \cdots + a_nx_n \mid a_1, \ldots, a_n \in A,\ x_1, \ldots, x_n \in X\}.$$

Teorema. 23.7.
Sea M un A-módulo. Si $\{N_i \mid i \in I\}$ es una familia de submódulos de M, existe un menor submódulo de M que contiene a cada elemento de la familia, que notaremos por $\sum\{N_i \mid i \in I\}$ y llamaremos ***suma de la familia****; la descripción a través de sus elementos es:*

$$\left\{\sum_j n_j \mid j \in F \subseteq I \text{ finito},\ n_j \in N_j \text{ para todo } j \in F\right\}.$$

Se tiene entonces que $\sum_i N_i$ es el ***supremo*** *de la familia $\{N_i \mid i \in I\}$.*

Lema. 23.8.
El conjunto $\mathcal{L}(M)$ con la relación de orden "$\leq$" es un ***retículo*** *con* ***ínfimo*** *la intersección y* ***supremo*** *la suma.*

Proposición. 23.9.
Sea $f : M \longrightarrow M'$ un homomorfismo de A-módulos, se verifican las siguientes propiedades:
(1) Si N es un submódulo de M, entonces $f(N)$ es un submódulo de M'.
(2) Si N' es un submódulo de M', entonces $f^{-1}(N')$ es un submódulo de M.
(3) Tanto f como f^{-1} son homomorfismos de retículos.

Tipos de homomorfismos

Sean M, M' dos A-módulos, el conjunto de los homomorfismos de A-módulos de M a M' se representa por $\mathrm{Hom}_A(M, M')$.

Lema. 23.10.
En la situación anterior $\mathrm{Hom}_A(M, M')$ es un A-módulo con operaciones definidas mediante:
(1) $(f+g)(m) = f(m) + g(m)$, para cualesquiera f, $g \in \mathrm{Hom}_A(M, M')$ y $m \in M$;
(2) $(af)(m) = a(f(m))$, para cualesquiera $a \in A, f \in \mathrm{Hom}_A(M, M')$ y $m \in M$.

Además si X e Y son A-módulos y $h : X \longrightarrow M$, $k : M' \longrightarrow Y$, son homomorfismos de A-módulos, entonces para $f, g \in \mathrm{Hom}_A(M, M')$

$$X \xrightarrow{h} M \underset{g}{\overset{f}{\rightrightarrows}} M' \xrightarrow{k} Y$$

se verifica:

$$(f+g)\circ h = f\circ h + g\circ h \qquad \text{y} \qquad k\circ(f+g) = k\circ f + k\circ g.$$

En particular tenemos que $\mathrm{End}_A(M)$ es un anillo, no necesariamente conmutativo, que es un subanillo de $\mathrm{End}(M)$, el anillo de los endomorfismos del grupo abeliano subyacente a M.

Observa que el anillo $\mathrm{End}_A(M)$ actúa a la derecha, por composición, sobre $\mathrm{Hom}_A(M, M')$ y que el anillo $\mathrm{End}_A(M')$ actúa a la izquierda sobre $\mathrm{Hom}_A(M, M')$, pero estas acciones no las vamos a utilizar en este texto.

Sea $f : M \longrightarrow M'$ un homomorfismo de A-módulos, la **imagen** de f es:

$$\mathrm{Im}(f) = \{f(m) \mid m \in M\},$$

y el **núcleo** de f es:

$$\mathrm{Ker}(f) = \{m \in M \mid f(m) = 0\}.$$

Lema. 23.11.
En la situación anterior $\mathrm{Im}(f)$ *y* $\mathrm{Ker}(f)$ *son submódulos de* M' *y* M *respectivamente.*

El cero de $\mathrm{Hom}_A(M, M')$ se representa por 0 y verifica: $\mathrm{Im}(0) = \{0\}$, $\mathrm{Ker}(0) = M$.

Teorema. 23.12.
En la situación anterior se verifica:

(1) f *es una aplicación inyectiva si, y sólo si,* $\mathrm{Ker}(f) = \{0\}$.
(2) f *es una aplicación sobreyectiva si, y sólo si,* $\mathrm{Im}(f) = M'$.
(3) f *es una aplicación biyectiva si, y sólo si, existe un homomorfismo* $g : M' \longrightarrow M$ *verificando* $f\circ g = id_{M'}$ *y* $g\circ f = id_M$.

Un homomorfismo de A-módulos verificando las condiciones del Teorema (23.12..3) se llama un **isomorfismo**. Para un A-módulo M un isomorfismo $f : M \longrightarrow M$ se llama **automorfismo**. El conjunto de los automorfismos de un A-módulo M se representa por $\mathrm{Aut}_A(M)$, y tiene estructura de grupo (no necesariamente abeliano) respecto a la composición, ya que es el conjunto de los elementos invertibles del anillo $\mathrm{End}_A(M)$.

Proposición. 23.13. (Propiedad universal del núcleo.)
Sea $f : M \longrightarrow M'$ un homomorfismo de A-módulos.

(1) Si $i : \operatorname{Ker}(f) \longrightarrow M$ es la inclusión, entonces la composición $i \circ f$ es cero, y
(2) si $g : X \longrightarrow M$ es un homomorfismo de A-módulos verificando $g \circ f = 0$, entonces existe un único homomorfismo de A-módulos $g' : X \longrightarrow \operatorname{Ker}(f)$ tal que $g = i \circ g'$.

$$\begin{array}{ccccc} \operatorname{Ker}(f) & \xrightarrow{i} & M & \xrightarrow{f} & M' \\ \uparrow {\scriptstyle \exists_1\, g'} & \nearrow {\scriptstyle g} & & & \\ X & & & & \end{array}$$

Un homomorfismo $f : M \longrightarrow M'$ con núcleo igual a cero se llama un **monomorfismo**. Observa que un homomorfismo f es un monomorfismo si y solo si es una aplicación inyectiva, y si, y sólo si, es simplificable a izquierda, esto es, si $f \circ g_1 = f \circ g_2$ para $g_1, g_2 : N \to M$, entonces $g_1 = g_2$.

24. Módulo cociente

Sea M un A-módulo y N un submódulo, consideramos el grupo cociente M/N y la proyección canónica $p : M \longrightarrow M/N$, entonces tenemos:

Lema. 24.1.
En la situación anterior existe una única estructura de A-módulo en M/N de forma que $p : M \longrightarrow M/N$ sea un homomorfismo de A-módulos.

El módulo M/N se llama **módulo cociente** de M por N.
Sea $f : M \longrightarrow M'$ un homomorfismo de A-módulos, llamamos **conúcleo** de f, y lo representamos por $\operatorname{Coker}(f)$, al módulo cociente $M'/\operatorname{Im}(f)$.

Proposición. 24.2. (Propiedad universal del conúcleo.)
En la situación anterior, supongamos que $p : M \longrightarrow \operatorname{Coker}(f)$ es la proyección canónica, entonces

(1) $p \circ f = 0$ y
(2) si $g : M' \longrightarrow Y$ es un homomorfismo verificando $g \circ f = 0$, entonces existe un único homomorfismo de A-módulos $g' : \operatorname{Coker}(f) \longrightarrow Y$ tal que $g = g' \circ p$.

$$\begin{array}{ccccc} M & \xrightarrow{f} & M' & \xrightarrow{p} & \operatorname{Coker}(f) \\ & & & \searrow^{g} & \downarrow{\scriptstyle exists_1\, g'} \\ & & & & Y \end{array}$$

Cuando f es la inclusión de un submódulo N' de M', entonces el conúcleo es precisamente el cociente de M' por N'.
Un homomorfismo $f : M \longrightarrow M'$ con conúcleo igual a cero se llama un **epimorfismo**. Observa que un homomorfismo f es un epimorfismo si y solo si es una aplicación sobreyectiva, y si, y sólo si, es simplificable a derecha, esto es, si $g_1 \circ f = g_2 \circ f$, para $g_1, g_2 : M' \to N$, entonces $g_1 = g_2$.
Es de destacar que las propiedades universales del núcleo y el conúcleo están expresadas para los pares $(\operatorname{Ker}(f), i)$ y $(p, \operatorname{Coker}(f))$ respectivamente. Por lo que desde un punto de vista formal la definición de núcleo y conúcleo de un homomorfismo hay que realizarla para los pares anteriormente citados. Siguiendo en esta línea, vamos a introducir nuevos ejemplos de construcciones universales en las siguientes secciones.
Vamos a hacer uso de los módulos cocientes en el estudio de módulos y homomorfismos de módulos.

Teoremas de isomorfía

Teorema. 24.3.
Dado un homomorfismo de A–módulos $f : M \longrightarrow M'$, se verifica:

(1) Existe una proyección $p : M \longrightarrow M/\operatorname{Ker}(f)$ definida por $p(m) = m + \operatorname{Ker}(f)$ para cada $m \in M$.
(2) Existe una inclusión $j : \operatorname{Im}(f) \longrightarrow M'$ definida por $j(f(m)) = f(m)$ para cada $m \in M$.
(3) ***Primer Teorema de Isomorfía.*** *Existe un isomorfismo $b : M/\operatorname{Ker}(f) \longrightarrow \operatorname{Im}(f)$ definido por $b(m + \operatorname{Ker}(f)) = f(m)$ para cada $m \in M$.*

$$\begin{array}{ccc} M & \xrightarrow{\quad f \quad} & M' \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle j} \\ M/\operatorname{Ker}(f) & \overset{\cong}{\underset{b}{-\,-\,\rightarrow}} & \operatorname{Im}(f) \end{array}$$

(4) Existe una biyección, que conserva el orden, entre las familias de submódulos

$$\mathcal{A} = \{N \subseteq M \mid \operatorname{Ker}(f) \subseteq N\} \text{ y}$$

$$\mathcal{B} = \{N' \subseteq M' \mid N' \subseteq \operatorname{Im}(f)\}.$$

En esta biyección la imagen de $N \in \mathcal{A}$ es $f_*(N) \subseteq M'$ y la imagen de $N' \in \mathcal{B}$ es $f^*(N') \subseteq M$

Teorema. 24.4. (Segundo Teorema de isomorfía o Teorema del paralelogramo)
Sea M un A-módulo y N_1, N_2 submódulos de M. Existe un isomorfismo

$$\frac{N_1}{N_1 \cap N_2} \cong \frac{N_1 + N_2}{N_2},$$

definido por $x + (N_1 \cap N_2) \mapsto x + N_2$.

$$\begin{array}{ccc} & & N_1 + N_2 \\ & \nearrow & \uparrow \\ N_1 & & N_2 \\ \uparrow & \nearrow & \\ N_1 \cap N_2 & & \end{array}$$

Tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccc}
N_1 \cap N_2 & \hookrightarrow & N_2 & \twoheadrightarrow & \frac{N_2}{N_1 \cap N_2} \\
\downarrow & & \downarrow & & \Vert \\
N_1 & \hookrightarrow & N_1 + N_2 & \twoheadrightarrow & \frac{N_1+N_2}{N_1} \\
\downarrow & & \downarrow & & \downarrow \\
\frac{N_1}{N_1 \cap N_2} & = & \frac{N_1+N_2}{N_2} & \longrightarrow & 0
\end{array}$$

Para completar la teoría vamos a incluir el Tercer Teorema de Isomorfía o del Doble Cociente.

Teorema. 24.5. (Tercer Teorema de Isomorfía. o Teorema del Doble Cociente)
Sean M un A–módulo y $N \subseteq L$ submódulos de M. Existe una biyección, que conserva el orden, entre los submódulos de M que contienen a N y los submódulos de M/N, dada por $L \mapsto \dfrac{L}{N}$. Además para cada $N \subseteq L \subseteq M$ existe un isomorfismo

$$\frac{M/N}{L/N} \cong \frac{M}{L},$$

que está definido por $m + M + \dfrac{L}{N} \mapsto m + L$.

Tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccccc}
N & \hookrightarrow & L & \twoheadrightarrow & L/N \\
\Vert & & \downarrow & & \downarrow \\
N & \hookrightarrow & M & \twoheadrightarrow & M/N \\
\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & L/M & = & \bullet
\end{array}$$

Los teoremas de isomorfía segundo y tercero se conocen como teoremas de **isomorfía de Noether**.

Módulos cíclicos

Si M es un A–módulo, para cada $m \in M$ podemos definir la aplicación $f_m : A \longrightarrow M$ mediante $f_m(a) = am$ para cada $a \in A$.

Lema. 24.6.
Sea M un A–módulo. Se verifica:

(1) Para cada $m \in M$ la aplicación $f_m : A \longrightarrow M$ es un homomorfismo A–módulos.
(2) El núcleo de f_m es $\{a \in A \mid am = 0\}$ se llama el **anulador** *de m, y se representa por $\operatorname{Ann}_A(m)$. Como consecuencia es un ideal de A.*
(3) El **anulador** *del módulo M se define como $\operatorname{Ann}_A(M) = \cap\{\operatorname{Ann}_A(m) \mid m \in M\}$.*

Ejercicio. 24.7.
Demuestra que cada A–módulo M tiene una estructura de módulo sobre el anillo $A/\operatorname{Ann}_A(M)$ de forma que la estructura de A–módulo inducida por el cambio de anillo, $A \to A/\operatorname{Ann}_A(M)$, coincide con la estructura original en M.

Recordar que un A–módulo es **cíclico** si está generado por un elemento.

Proposición. 24.8.
Dado un A–módulo cíclico M con generador $g \in M$, se tiene:

(1) El homomorfismo $f_g : A \longrightarrow M$ es sobreyectivo.
(2) Existe un isomorfismo $A/\operatorname{Ann}_A(g) \cong M$.

Como consecuencia todo A–módulo cíclico es un cociente del anillo A.

25. Suma directa de A–módulos

Sea $\{M_i \mid i \in I\}$ una familia de A-módulos, se llama **suma directa** de la familia a un A-módulo M junto con una familia de homomorfismos de A-módulos $\{j_i : M_i \longrightarrow M \mid i \in I\}$ verificando: *para cada A-módulo X y cada familia de homomorfismos de A-módulos $\{f_i : M_i \longrightarrow X \mid i \in I\}$, existe un único homomorfismo de A-módulos $f : M \longrightarrow X$ tal que $f_i = f \circ j_i$ para cada índice $i \in I$*, esto es, los siguientes diagramas son conmutativos para todo $i \in I$.

$$\begin{array}{ccc} M_i & \xrightarrow{j_i} & M \\ & \searrow^{f_i} & \downarrow \exists_1 f \\ & & X \end{array}$$

Esto significa que cada familia de homomorfismos de los M_i a un módulo dado X se *factoriza* a través de M por los j_i.

La suma directa, si existe, es única salvo isomorfismo, esto es, si el par $(Y, \{h_i : M_i \longrightarrow Y \mid i \in I\})$ es otra suma directa de la misma familia, entonces existe un isomorfismo $h : M \longrightarrow Y$ tal que $h_i = h \circ j_i$ para cada $i \in I$; esto es, los siguientes diagramas son conmutativos para todo $i \in I$.

$$\begin{array}{ccc} M_i & \xrightarrow{j_i} & M \\ & \searrow^{h_i} & \downarrow h \\ & & Y \end{array}$$

Dada una familia de A-módulos vamos a construir una suma directa. Para ello definimos

$$M = \oplus\{M_i \mid i \in I\} \subseteq \prod\{M_i \mid i \in I\},$$

formado por los elementos de soporte finito, y $j_k : M_k \longrightarrow \oplus_i M_i$ mediante: $j_k(x) = (\delta_{k,i}x)_i$, para cada $k \in I$. El par $(\oplus M_i, \{j_i \mid i \in I\})$ es una suma directa de la familia $\{M_i \mid i \in I\}$.

Por abuso de lenguaje, al igual que en el caso del núcleo y el conúcleo, se llama **suma directa** de la familia al A-módulo $\oplus_i M_i$, sobre-entendiendo los homomorfismos j_i.

Veamos ahora algunas propiedades de la suma directa:

Proposición. 25.1.

(1) *Para cada $i \in I$ el homomorfismo $j_i : M_i \to \oplus_i M_i$ es un monomorfismo;*

(2) *Sean $\{M_i \mid i \in I\}$ y $\{N_i \mid i \in I\}$ familias de A–módulos de forma que para cada índice $i \in I$ existe un homomorfismo de A–módulos $f_i : N_i \longrightarrow M_i$. Existe un único homomorfismo $f : \oplus_i N_i \longrightarrow \oplus_i M_i$ tal que $j_i \circ f_i = f \circ h_i$ para cada $i \in I$, siendo $h_i : N_i \longrightarrow \oplus_i N_i$ la inclusión canónica de N_i en la suma directa;*

$$\begin{array}{ccc} N_i & \xrightarrow{h_i} & \oplus_i N_i \\ f_i \downarrow & & \downarrow f \\ M_i & \xrightarrow{j_i} & \oplus_i M_i \end{array}$$

(3) Con la notación anterior, si cada f_i es un monomorfismo, resp. epimorfismo, entonces f es un monomorfismo, resp. epimorfismo;

(4) Si cada N_i es un submódulo de M_i, existe un isomorfismo $\oplus_i(M_i/N_i) \cong \dfrac{\oplus_i M_i}{\oplus_i N_i}$.

El concepto dual al de suma directa es el de **producto directo**.

Ejercicio. 25.2.
Desarrolla el concepto de producto directo y sus propiedades de forma análoga a como hemos hecho con la suma directa.

Sumas directas finitas

Sea $M_1, \ldots, M_t$ una familia finita de A–módulos. Podemos considerar la suma directa $\oplus\{M_i \mid i = 1, \ldots, t\} = M_1 \oplus \cdots \oplus M_t$. Observar que junto a los homomorfismos $j_i : M_i \longrightarrow \oplus_i M_i$ tenemos otros definidos por

$$p_i : \oplus_i M_i \longrightarrow M_i, \quad p_i(m_1, \ldots, m_t) = m_i.$$

Es fácil ver que $(\oplus_i M_i, \{p_i \mid i = 1, \ldots, t\})$ es un producto directo de la familia.
Los homomorfismos j_i y p_i verifican, entre otras, las siguientes relaciones:

$$\begin{array}{ll} p_i \circ j_i = \mathrm{id}_{M_i}, & \forall i = 1, \ldots, t \\ p_i \circ j_h = 0, & \text{si } i \neq h \\ j_1 p_1 + \cdots + j_t p_t = \mathrm{id}_M . & \end{array}$$

Podemos entonces enunciar y probar el siguiente

Teorema. 25.3.
Sea $M, M_1, \ldots, M_t$ una familia finita de A–módulos y $\{j_i : M_i \longrightarrow M \mid i = 1, \ldots, t\}$ una familia finita de homomorfismos. Son equivalentes

(a) $(M, \{j_i \mid i = 1, \ldots, t\})$ es una suma directa.

(b) Existe una familia de homomorfismos $\{p_i : M \longrightarrow M_i \mid i = 1, \ldots, t\}$ tal que $p_i \circ j_h = \delta_{i,h}\, \mathrm{id}_{M_i}$ y $\sum_{i=1}^{t} j_i \circ p_i = \mathrm{id}_M$.

De forma dual podemos enunciar este Teorema para productos directos.

Ejercicio. 25.4.
Enunciar y probar el Teorema (25.3.) para productos directos.

Homomorfismos

En el caso de tratar con homomorfismos entre dos sumas directas de familias finitas de módulos, el uso de matrices es muy útil como vamos a ver a continuación.

Proposición. 25.5.
Dadas dos familias finitas de A–módulos $\{M_i \mid i = 1, \ldots, t\}$ y $\{N_h \mid h = 1, \ldots, s\}$, existe un isomorfismo

$$\mathrm{Hom}_A(\oplus_{i=1}^t M_i, \oplus_{h=1}^s N_h) \cong \oplus_{i=1}^t \oplus_{h=1}^s \mathrm{Hom}_A(M_i, N_h),$$

que a cada homomorfismo $f : \oplus_{i=1}^t M_i \longrightarrow \oplus_{h=1}^s N_h$ hace corresponder $(f_{hi})_{hi}$, donde $f_{hi} : M_i \longrightarrow N_h$ está definido $f_{hi}(x) = (p_h \circ f \circ j_i)(x)$.

DEMOSTRACIÓN. Vamos a construir la aplicación inversa. Dado $(f_{hi})_{hi}$, para cada índice i consideramos $\{f_{hi} \mid h = 1, \ldots, s\}$, que inducen un homomorfismo $f_i : M_i \longrightarrow \prod_h N_h$. Ahora consideramos la familia $\{f_i \mid i = 1, \ldots, t\}$, que induce un homomorfismo $\oplus_i M_i \longrightarrow \prod_h N_h$, que es el morfismo f inicial. □

El homomorfismo $f : \oplus_{i=1}^t M_i \longrightarrow \oplus_{h=1}^s N_h$ puede ahora representarse por la matriz $(f_{hi})_{hi}$, y la imagen de un elemento $(m_1, \ldots, m_t) \in \oplus_i M_i$ se expresa:

$$\begin{pmatrix} f_{11} & \cdots & f_{1t} \\ \vdots & \ddots & \vdots \\ f_{s1} & \cdots & f_{st} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_t \end{pmatrix} = \begin{pmatrix} \sum_i f_{1i}(m_i) \\ \vdots \\ \sum_i f_{si}(m_i) \end{pmatrix} \in \oplus_{h=1}^s N_h.$$

Suma directa interna

Se considera ahora un A–módulo M y una familia finita de submódulos: $N_1, \ldots, N_t$. Estamos interesados en relacionar $\oplus_{i=1}^t N_i$ y M.
Por la propiedad universal de la suma directa tenemos un homomorfismo $f : \oplus_{i=1}^t N_i \longrightarrow M$, inducido por las inclusiones $N_i \subseteq M$, y definido por: $f((n_i)_i) = \sum_{i=1}^t n_i$.

Lema. 25.6.
Con la notación anterior se verifica:

(1) f es sobreyectivo si, y solo si, $\sum_{i=1}^{t} N_i = M$ y
(2) f es inyectivo si, y solo si, $N_h \cap (N_1 + \cdots + N_{h-1} + N_{h+1} + \cdots + N_t) = 0$ para cada índice h, si, y solo si, $N_h \cap (N_1 + \cdots + N_{h-1}) = 0$ para cada índice h.

Cuando f es un isomorfismo decimos que M es la **suma directa interna** de los $N_1, \ldots, N_t$.

Una familia finita de submódulos $N_1, \ldots, N_t \subseteq M$ se dice **independiente** si verifica las condiciones equivalentes del apartado (2) Lema (25.6.).

Observa que la condición (2) del Lema (25.6.) es necesaria, y que no basta que cada intersección $N_i \cap N_j$, con $i \neq j$, se nula. Estudia el ejemplo $\mathbb{Z}_2 \times \mathbb{Z}_2$.

26. Módulos libres

Un A-módulo F se llama **libre** sobre un subconjunto $X \subseteq F$ si para cada aplicación $f : X \longrightarrow M$, de X en un A-módulo M, existe un único homomorfismo $f' : F \longrightarrow M$ tal que $f'_{|X} = f$.

$$\begin{array}{ccc} X & \xrightarrow{incl.} & F \\ & \searrow^{f} & \downarrow \exists_1 f' \\ & & M \end{array}$$

El conjunto X se llama una **base** de F.

Lema. 26.1.
Si F es libre sobre X y G es libre sobre Y y existe una aplicación de $f : X \longrightarrow Y$, entonces f induce un homomorfismo de $\overline{f} : F \longrightarrow G$. Si f es una biyección, entonces $\overline{f}$ es un isomorfismo.

$$\begin{array}{ccc} X & \hookrightarrow & F \\ f\downarrow & & \downarrow \overline{f} \\ Y & \hookrightarrow & G \end{array}$$

Como consecuencia, sobre cada conjunto X existe, salvo isomorfismo, un único módulo libre. Observar que estos módulos son isomorfos para cada par de conjuntos con el mismo cardinal.

Dado un conjunto X existe siempre un A–módulo libre sobre X. Para construirlo definimos $F = \oplus\{A_x \mid x \in X,\ A_x = A,\ \text{para todo } x \in X\}$ e $i : X \longrightarrow F$ mediante $i(x) = e_x$, donde $e_x = (\delta_{x,y})_y$. De esta forma podemos identificar X con el conjunto $\{e_x \mid x \in X\}$.

Proposición. 26.2.
Con la notación anterior F es libre sobre X.

Como consecuencia de esta construcción, y de la definición de módulo libre, resulta que cada A–módulo libre sobre un conjunto X es isomorfo a una suma directa, indizada en X, de copias del anillo A.

Una propiedad importante de los módulo libres es:

Teorema. 26.3.
Cada A–módulo es un cociente de un A–módulo libre, y por tanto de una suma directa de copias de A.

Dado un A–módulo M una **presentación libre** de M es dar un módulo libre F y un submódulo K tal que $F/K \cong M$, o equivalentemente dar un homomorfismo sobreyectivo de un módulo libre a M.

Una presentación libre se llama **finita** cuando tanto F con K son finitamente generados. En este caso si F está generado por $\{f_1, \dots, f_t\}$ y K está generado por $\{k_1, \dots, k_s\}$, siendo $k_j = \sum_i a_i f_i$, representamos el módulo M como $M = \langle f_1, \dots, f_t \mid \sum_i a_i f_i = 0 \rangle$.

En particular un A–módulo es finitamente generado si, y sólo si, es un cociente de una suma directa finita de copias de A y advierte que un módulo finitamente generado no tiene que tener una presentación libre finita.

Si F es un A–módulo libre sobre un conjunto X y $\mathfrak{m}$ es un ideal maximal de A, en $F \cong A^{(X)}$ podemos considerar el submódulo $\mathfrak{m}A^{(X)}$; es claro que tenemos

$$\frac{A^{(X)}}{\mathfrak{m}A^{(X)}} = \frac{A^{(X)}}{\mathfrak{m}^{(X)}} \cong \left(\frac{A}{\mathfrak{m}}\right)^{(X)},$$

que es un $A/\mathfrak{m}$–espacio vectorial de dimensión $\mathrm{Card}(X)$. Como consecuencia si F es A–módulo libre sobre un conjunto X resulta que $\mathrm{Card}(X)$ es un invariante de F al que vamos a llamar el **rango** de F.

Esto completa el resultado al inicio de esta sección, de forma que, sobre un anillo conmutativo, a cada número cardinal podemos asociar una única clase de isomorfía de módulos libres de forma que esta correspondencia sea biyectiva.

Homomorfismos entre módulos libres finitamente generados

Cada A–módulo libre finitamente generado F es isomorfo a una suma directa A^n de copias del anillo A, por lo que el estudio de los homomorfismos entre dos A–módulos libres finitamente generados se reduce al estudio de homomorfismos entre sumas directas finitas de copias de A. Observa que el isomorfismo $F \cong A^n$ se establece fijando una base de F, por lo que tomando bases distintas podemos tener isomorfismos $F \cong A^n$ distintos.

Como cada endomorfismo de A está definido por un elemento $a \in A$, en virtud de la Proposición (25.5.) el estudio de los endomorfismos entre módulos libres finitamente generados se reduce al estudio de matrices con coeficientes en A.

Representamos por $M_{n\times m}(A)$ el conjunto de las matrices con coeficientes en A con n filas y m columnas. Por simplicidad el conjunto $M_{n\times n}(A)$ se representa por $M_n(A)$. Un elemento de $M_{n\times m}(A)$ se representa por

$$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}$$

El conjunto $M_{n\times m}(A)$ tiene estructura de A–módulo y el conjunto $M_n(A)$ tiene estructura de A–álgebra, aunque no conmutativa.

Al considerar la estructura multiplicativa de $M_n(A)$ aparece de forma natural el **grupo lineal general**, $GL_n(A)$, que es el grupo de las matrices invertibles.

Lema. 26.4.
Dadas dos matrices X e Y en $M_{n\times m}(A)$ que representan el mismo endomorfismo respecto a distintas bases, existen matrices invertibles $P \in M_n(A)$ y $Q \in M_m(A)$ tales que $X = PYQ$.

Dos matrices X e Y en la situación del lema se llaman matrices **equivalentes**. Es claro que la relación “equivalente a" es una relación de equivalencia en $M_{n\times m}(A)$.

Lema. 26.5.
Dadas dos matrices X e Y en $M_n(A)$, que representan el mismo endomorfismo respecto a distintas bases, existe una matriz invertible P tal que $Y = PXP^{-1}$.

Dos matrices X e Y en la situación del lema se llaman matrices **semejantes**. Es claro que la relación “semejante a" es una relación de equivalencia en $M_n(A)$.
Dada una matriz $X = (x_{ij})_{ij} \in M_n(A)$, el **determinante** de X se define

$$\det(X) = \sum_{\sigma\in S_n} (-1)^{s(\sigma)} a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

El determinante de una matriz X verifica algunas propiedades geométricas que son de interés. Dada X el **elemento adjunto** o **cofactor** de x_{ij} es el determinante de la matriz obtenida de X eliminando la fila i y la columna j, es pues el determinante de una matriz $(n-1)\times(n-1)$, afectado por el signo $(-1)^{i+j}$; se representa por X_{ij}. La **matriz adjunta** de la matriz X es la matriz $\mathrm{adj}(X) = (X_{ij})_{ji}$, esto es, la matriz traspuesta de la matriz formada por los elementos adjuntos.

Lema. 26.6. (Teorema de Laplace)
Dada una matriz $X = (x_{ij})_{ij} \in M_n(A)$, se verifica:
(1) $\det(X) = x_{i1}X_{i1} + \cdots + x_{in}X_{in}$ *para cada índice* $i = 1, \ldots, n$.
(2) $\det(X) = x_{1j}X_{1j} + \cdots + x_{nj}X_{nj}$ *para cada índice* $j = 1, \ldots, n$.
(3) $X\ adj(X) = \det(X)\ I = adj(X)\ X$.

Corolario. 26.7.
Una matrix $X \in M_n(A)$ es invertible si, y solo si, $\det(X)$ es un elemento invertible en A.

27. Módulos finitamente generados

Lema. 27.1. (Teorema de Cayley–Hamilton.)
Sea M un A–módulo finitamente generado, $\mathfrak{a}$ un ideal de A y f un endomorfismo de M tal que $f(M) \subseteq \mathfrak{a}M$. Entonces f verifica una ecuación de la forma

$$f^n + a_1 f^{n-1} + \cdots + a_{n-1} f + a_n = 0, \text{ con } a_i \in \mathfrak{a}.$$

DEMOSTRACIÓN. Sea $\{m_1, \ldots, m_t\} \subseteq M$ un sistema de generadores de M, y sea $f(m_i) = \sum_{j=1}^{t} a_{ij} m_j$, con $a_{ij} \in \mathfrak{a}$. Tenemos entonces

$$\sum_{j=1}^{t} (\delta_{i,j} f - a_{ij}) m_j = 0.$$

Multiplicamos por la derecha por la adjunta de $(\delta_{i,j} f - a_{ij})_{ij}$, obteniendo que $\det(\delta_{i,j} f - a_{ij})_{ij}$ anula a cada m_j. Luego $\det(\delta_{i,j} f - a_{ij})_{ij}$ es el homomorfismo cero y al desarrollar se tiene la ecuación buscada.
OTRA DEMOSTRACIÓN.
Se considera el diagrama:

$$\begin{array}{ccccccc}
\mathrm{Ker}(f') & \longrightarrow & A^t & \xrightarrow{f'} & \mathfrak{a}A^t & \xrightarrow{incl} & A^t \\
\downarrow & & \downarrow \rho & & \downarrow \rho & & \downarrow \rho \\
\mathrm{Ker}(f) & \longrightarrow & M & \xrightarrow{f} & \mathfrak{a}M & \xrightarrow{incl} & M
\end{array}$$

donde $\rho : A^t \longrightarrow M$ es la proyección canónica y $f' : A^t \longrightarrow \mathfrak{a}A^t$ está definida por $f(e_i) = \sum_{j=1}^{t} a_{ij} e_j$, siguiendo la notación anterior, esto es, $f(m_i) = \sum_{j=1}^{t} a_{ij} m_j$, con $a_{ij} \in \mathfrak{a}$. El diagrama es conmutativo y $f' : A^t \longrightarrow A^t$ está definido por una matriz; sea ésta E. La matriz E es raíz de su polinomio característico: $\det(E - \lambda I)$. Sustituyendo E por f tenemos la ecuación buscada. □

Corolario. 27.2.
Sea M un A–módulo finitamente generado y $\mathfrak{a}$ un ideal de A tal que $\mathfrak{a}M = M$. Entonces existe un $x \in A$ tal que $x \equiv 1 \pmod{\mathfrak{a}}$ y $xM = 0$.

DEMOSTRACIÓN. Si tomamos en el Lema (27.1.) $f = \mathrm{id}_M$, para cada $m \in M$ se verifica $(1 + a_1 + \cdots + a_{n-1} + a_n)m = 0$. Por lo tanto podemos tomar $x = 1 + a_1 + \cdots + a_{n-1} + a_n$ que cumple las dos condiciones del enunciado. □

Lema. 27.3. (Lema de Nakayama.)
Sea M un A–módulo finitamente generado y $\mathfrak{a}$ un ideal de A contenido en $\operatorname{Rad}(A)$. Entonces $\mathfrak{a}M = M$ implica $M = 0$.

DEMOSTRACIÓN. Por el Corolario (27.2.) existe $x \in A$ tal que $x \equiv 1 \pmod{\mathfrak{a}}$ y $xM = 0$. Como $x - 1 \in \mathfrak{a} \subseteq \operatorname{Rad}(A)$, entonces $x \in A$ es una unidad, entonces $M = 0$.
OTRA DEMOSTRACIÓN.
Si $M \neq 0$, consideramos un conjunto minimal de generadores de M, por ejemplo $\{m_1, \ldots, m_t\}$. Para cada m_i tenemos una expresión del tipo

$$m_i = \sum_{j=1}^{t} a_{ij} m_j, \qquad \text{con } a_{ij} \in \mathfrak{a} \subseteq \operatorname{Rad}(a).$$

Entonces se verifica

$$(1 - a_{tt}) m_t = \sum_{j=1}^{t-1} a_{ij} m_j,$$

y como $1 - a_{tt}$ es una unidad, resulta que $\{m_1, \ldots, m_{t-1}\}$ es un sistema de generadores, lo que es una contradicción. □

Corolario. 27.4.
Sea M un A–módulo finitamente generado, N un submódulo de M, $\mathfrak{a}$ un ideal de A contenido en $\operatorname{Rad}(A)$. Entonces $\mathfrak{a}M + N = M$ implica $N = M$.

En realidad solo necesitamos que el cociente M/N sea finitamente generado.

DEMOSTRACIÓN. Basta tomar el módulo finitamente generado M/N en el Lema de Nakayama, ya que se tiene $\mathfrak{a}\left(\frac{M}{N}\right) = \frac{\mathfrak{a}M+N}{N}$. □

Lema. 27.5.
Sea $(A, \mathfrak{m})$ un anillo local y M un A–módulo finitamente generado. Si $x_1, \ldots, x_t$ son elementos de M tales que sus clases en $M/\mathfrak{m}M$ generan $M/\mathfrak{m}M$ como $A/\mathfrak{m}$–módulo. Entonces $\{x_1, \ldots, x_t\}$ es un sistema de generadores de M.

DEMOSTRACIÓN. Tomamos en el Corolario (27.4.) $N = Ax_1 + \cdots + Ax_t$. □

Si M es un A–módulo finitamente generado, llamamos $\mu(M)$ al menor número de elementos de un sistema de generadores de M. Un sistema de generadores con $\mu(M)$ elementos se llama un **sistema de generadores minimal**.

Consecuencia de la definición de rango de un módulo libre tenemos:

Lema. 27.6.
Si F es un A–módulo libre finitamente generado, entonces $\mu(F)$ es el número de elementos de una base, esto es, el rango de F.

DEMOSTRACIÓN. Sea s el rango de F y $\{m_1,\ldots,m_t\}$ un sistema minimal de generadores, para cada ideal maximal $\mathfrak{m}$ se tiene que $\{\overline{m_1},\ldots,\overline{m_t}\}$ es un sistema de generadores de $F/\mathfrak{m}F$. Como $F/\mathfrak{m}F \cong \left(\frac{A}{\mathfrak{m}}\right)^t$, tenemos $t \leq m$, y en consecuencia $t = s$, el rango de F. □

Este resultado se puede aplicar ahora a anillos locales y obtenemos:

Corolario. 27.7.
Sea $(A,\mathfrak{m},K)$ un anillo local y M un A–módulo finitamente generado. Si m_1, ..., $m_t \in M$, son equivalentes:

(a) $M = Am_1 + \cdots + Am_t$;
(b) $\{\overline{m_1},\ldots,\overline{m_t}\} \subseteq M/\mathfrak{m}M$ es un sistema de generadores $M/\mathfrak{m}M$ como K–espacio vectorial.

Corolario. 27.8.
Con las mismas hipótesis se verifica:

(1) $\mu = \dim_K(M/\mathfrak{m}M)$;
(2) $m_1,\ldots,m_n$ es un sistema minimal de generadores de M si, y sólo si, $\{\overline{m_1},\ldots,\overline{m_n}\}$ es una K–base de $M/\mathfrak{m}M$;
(3) si $m_1,\ldots,m_n$ es un sistema minimal de generadores de M y $\sum_{i=1}^n r_im_i = 0$, $r_i \in A$, entonces $r_i \in \mathfrak{m}$ para cada índice i;
(4) cada sistema de generadores contiene uno minimal;
(5) los elementos m_1, ..., m_n pueden extenderse a un sistema minimal de generadores de M si, y sólo si, $\{\overline{m_1},\ldots,\overline{m_n}\}$ son K–linealmente independientes en $M/\mathfrak{m}M$ sobre el cuerpo $A/\mathfrak{m}$.

28. Módulos noetherianos

Un A–módulo M verifica la **condición maximal** si toda familia no vacía de submódulos, ordenada por inclusión, tiene un elemento maximal.

Un A–módulo M verifica la **condición de cadena ascendente** si toda cadena ascendente de submódulos de M es estacionaria, esto es, si $M_1 \subseteq M_2 \subseteq \cdots$ es una cadena ascendente de submódulos de M, entonces existe $m \in \mathbb{N}$ tal que $M_m = M_n$ para todo $n \geq m$.

Un A–módulo M se llama **noetheriano** si es finitamente generado y cada submódulo N de M es finitamente generado.

Lema. 28.1.
Sea M un A–módulo, son equivalentes los siguientes enunciados:

(a) M es noetheriano.
(b) M verifica la condición maximal.
(c) M verifica la condición de cadena ascendente.

DEMOSTRACIÓN. (a)⇒(b). Sea Γ una familia no vacía de submódulos de M. Sea $M_0 \subseteq M_1 \subseteq \cdots$ una cadena de elementos de Γ, entonces $\cup_i M_i$ es un submódulo finitamente generado de M por ser M noetheriano. Si $\{m_1, \ldots, m_t\}$ es un sistema de generadores de $\cup_i M_i$, existe un índice j tal que $\{m_1, \ldots, m_t\} \subseteq M_j$, y por tanto $\cup_i M_i = M_j \in \Gamma$. Así pues, por el Lema de Zorn, Γ tiene elementos maximales.

(b)⇒(c). Si $M_0 \subseteq M_1 \subseteq \cdots$ es una cadena ascendente de submódulos de M, entonces la familia $\{M_0, M_1, \ldots\}$ tiene un elemento maximal, sea M_j, por tanto para $h > j$ se verifica $M_h = M_j$ y la cadena es estacionaria.

(c)⇒(a). Si N es un submódulo de M, consideramos un elemento $n_1 \in N$. Si $n_1 A = N$, entonces N es finitamente generado. En caso contrario existe $n_2 \in N \setminus n_1 A$. Si $n_1 A + n_2 A = N$, entonces N es finitamente generado. En caso contrario existe $n_3 \in N \setminus n_1 A + n_2 A$ .... Si para cada índice i podemos encontrar un elemento $n_{i+1} \in N \setminus n_1 A + \cdots + n_i A$, entonces podemos construir una cadena estrictamente ascendente

$$n_1 A \subset n_1 A + n_2 A \subset \cdots \subset n_1 A + \cdots + n_i A \subset \cdots ,$$

lo que es una contradicción. □

Lema. 28.2.
Sea $0 \to M' \to M \to M'' \to 0$ una sucesión exacta corta de A–módulos. Son equivalentes los siguientes enunciados:

(a) M es noetheriano.
(b) M' y M'' son noetherianos.

DEMOSTRACIÓN. (a)⇒(b). Ya que cada cadena de submódulos de M' es también una cadena de submódulos de M, tenemos que cada cadena de submódulos de M' estabiliza. Si $M''_1 \subset M''_2 \subseteq \cdots$ es una cadena de submódulos de M'', entonces identificando M'' con M/M', tenemos que existe una cadena

$$M_1 \subseteq M_1 \subseteq \cdots$$

de submódulos de M, en donde $M_i/M' = M''_i$ para cada índice i. Como la cadena de submódulos de M estabiliza, entonces la cadena $M''_1 \subset M''_2 \subseteq \cdots$ también estabiliza. □

Como consecuencia tenemos el siguiente resultado.

Corolario. 28.3.
Cada submódulo y cada cociente de un A–módulo noetheriano es noetheriano y una suma directa finita de A–módulos es noetheriana si, y solo si, cada sumando es noetheriano.

Módulos artinianos

Un A–módulo M verifica la **condición minimal** si toda familia no vacía de submódulos, ordenada por inclusión, tiene un elemento minimal.

Un A–módulo M verifica la **condición de cadena descendente** si toda cadena descendente de submódulos de M es estacionaria, esto es, si $M_1 \supseteq M_2 \supseteq \cdots$ es una cadena descendente de submódulos de M, entonces existe $m \in \mathbb{N}$ tal que $M_m = M_n$ para todo $n \geq m$.

Lema. 28.4.
Sea M un A–módulo, son equivalentes los siguientes enunciados:

(a) M verifica la condición minimal.
(b) M verifica la condición de cadena descendente.

Un A–módulo M que verifica las condiciones equivalentes del Lema se llama **artiniano**.

Como consecuencia tenemos el siguiente resultado.

Corolario. 28.5.
Cada submódulo y cada cociente de un A–módulo artiniano es artiniano y una suma directa finita de A–módulos es artiniana si, y solo si, cada sumando es artiniano.

Anillos noetherianos

Un anillo A se llama **noetheriano** si ${}_AA$ es un A–módulo noetheriano.

Lema. 28.6.
Sea A un anillo, son equivalentes los siguientes enunciados:

(a) A es noetheriano.
(b) Cada A–módulo finitamente generado es noetheriano.

DEMOSTRACIÓN. (a)⇒(b). Si M es un A–módulo finitamente generado, entonces existe una presentación libre $A^n \to M \to 0$, y como A es noetheriano, entonces M lo es.
(b)⇒(a). Como ${}_AA$ es un A–módulo finitamente generado, tenemos que ${}_AA$ es noetheriano y por tanto A es un anillo noetheriano. □

Lema. 28.7.
Si A es un anillo noetheriano y $\mathfrak{a}$ es un ideal, entonces $A/\mathfrak{a}$ es un anillo noetheriano.

DEMOSTRACIÓN. Si $\mathfrak{b}$ es un ideal de $A/\mathfrak{a}$, entonces existe un ideal $\mathfrak{b}'$ de A tal que $\mathfrak{b} = \mathfrak{b}'/\mathfrak{a}$, y por tanto, como $\mathfrak{b}'$ es finitamente generado, resulta que $\mathfrak{b}$ también lo es. □

Existen más formas de construir anillos noetherianos a partir de otros que ya lo son. Veamos algunos ejemplos.

Proposición. 28.8. (Teorema de la base de Hilbert.)
Si A es un anillo noetheriano, el anillo de polinomios $A[X]$ es un anillo noetheriano.

DEMOSTRACIÓN. Sea $\mathfrak{a}$ un ideal de $A[X]$. Consideramos el conjunto de los coeficientes líderes de los polinomios en $\mathfrak{a}$. Este conjunto es un ideal de A, llamémoslo $\mathfrak{b}$. Ya que A es un anillo noetheriano, $\mathfrak{b}$ es un ideal finitamente generado. Supongamos que $\mathfrak{b} = a_1A + \cdots + a_tA$ y sea $F_i \in \mathfrak{a}$ tal que

$$F_i = a_iX^{n_i} + \text{términos de grado menor.}$$

Sea $\mathfrak{a}'$ el ideal de $A[X]$ generado por $F_1, \ldots, F_t$. Es claro que $\mathfrak{a}' \subseteq \mathfrak{a}$.
Sea $F = aX^m +$ términos de grado menor $\in \mathfrak{a}$. Si $m \geq n = \max\{n_i \mid i = 1, \ldots, t\}$, entonces consideramos una combinación tal que $a = \sum_{i=1}^{t} r_ia_i$ y construimos entonces

$$G = F - \sum_{i=1}^{t} r_iF_iX^{m-n_i} \in \mathfrak{a}.$$

Resulta que $\mathrm{gr}(G) < \mathrm{gr}(F)$. Luego reiterando este proceso el número de veces que sea necesario podemos suponer que $\mathrm{gr}(F) < n$.

Sea M el A–módulo generado por $1, X, \ldots, X^{n-1}$, entonces $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Por ser M finitamente generado es noetheriano y entonces $\mathfrak{a} \cap M$ es finitamente generado. Sean $G_1,\ldots,G_s$ una familia de generadores de $\mathfrak{a} \cap M$, entonces $\mathfrak{a}$ está generado como $A[X]$–módulo por $G_1, \ldots, G_s, F_1, \ldots, F_t$, y tenemos que es finitamente generado. □

Corolario. 28.9.
Si A es un anillo noetheriano, el anillo de polinomios $A[X_1, \ldots, X_n]$ es noetheriano.

Corolario. 28.10.
Sea A un anillo noetheriano y B una A–álgebra finitamente generada, entonces B es noetheriana. En particular toda álgebra finitamente generada sobre un cuerpo es noetheriana.

Caracterizaciones y ejemplos de anillos noetherianos[1]

Teorema. 28.11. (Teorema de Cohen.[4])
Sea A un anillo. Son equivalentes los siguientes enunciados:

(a) A es un anillo noetheriano.

(b) Todos los ideales primos de A son finitamente generados.

DEMOSTRACIÓN. (Matsumura:1986, pag. 17) (b)⇒(a). Llamamos Γ al conjunto de todos los ideales de A que no son finitamente generados. Si $\Gamma \neq \varnothing$, aplicando el Lema de Zorn existen en Γ elementos maximales. Sea $\mathfrak{a} \in \Gamma$ maximal. Si $\mathfrak{a}$ no es primo, existen $a, b \in A$ tales que $ab \in \mathfrak{a}$ y $a, b \notin \mathfrak{a}$. Consideramos $\mathfrak{a} + aA$; es finitamente generado ya que no pertenece a Γ. Entonces existen $a_1, \ldots, a_t \in \mathfrak{a}$ tales que $\mathfrak{a} + aA = a_1A + \cdots + a_tA + aA$.

Consideramos $(\mathfrak{a} : a)$. Tenemos que $\mathfrak{a} \subseteq (\mathfrak{a} : a)$, como $b \in (\mathfrak{a} : a) \setminus \mathfrak{a}$, entonces $(\mathfrak{a} : a) \notin \Gamma$ y es también finitamente generado. Entonces $(\mathfrak{a} : a) = b_1A + \cdots + b_mA$.

[1] OPCIONAL

Dado $y \in \mathfrak{a}$, existe una expresión

$$y = a_1 r_i + \cdots + a_t r_t + ar \text{ con } r_1, \ldots, r_t, r \in A.$$

Entonces $r \in (\mathfrak{a} : a)$ y existen $s_1, \ldots, s_m \in A$ tales que

$$r = b_1 s_1 + \cdots + b_m s_m,$$

Uniendo todo resulta

$$y = a_1 r_1 + \cdots + a_t r_t + ab_1 s_1 + \cdots + ab_m s_m,$$

y por tanto $\{a_1, \ldots, a_r, ab_1, \ldots, ab_m\}$ es un sistema de generadores de $\mathfrak{a}$, lo que es una contradicción. Resulta pues que Γ ha de ser vacío y por tanto A es un anillo noetheriano. □

Teorema. 28.12. (Teorema de la base de Hilbert para series formales de potencias.)
Sea A un anillo noetheriano y X una indeterminada, el anillo de series formales de potencias $A[[X]]$ es noetheriano.

DEMOSTRACIÓN. Sea $\mathfrak{a}$ un ideal de $A[[X]]$, llamamos $\mathfrak{a}_0$ al ideal de A formado por los términos independientes de los elementos de $\mathfrak{a}$. De forma similar llamamos $\mathfrak{a}_1$ al conjunto de los coeficientes de X en los elementos de $\mathfrak{a}$; es claro que $\mathfrak{a}_1$ es un ideal de A. De forma análoga definimos $\mathfrak{a}_h$ el ideal de los coeficientes de X_h en los elementos de $\mathfrak{a}$. Multiplicando por X tenemos $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$; por tanto tenemos una cadena de ideales de A:

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots$$

Esta cadena estabiliza, sea $\mathfrak{a}_t = \mathfrak{a}_{t+1} = \cdots$ Sea $\{a_{i,1}, \ldots, a_{i,s_i}\}$ un sistema de generadores de $\mathfrak{a}_i$ y sea $F_{i,j} \in \mathfrak{a}$ una serie tal que el coeficiente de X^i es $a_{i,j}$. Veamos que $\{F_{i,j} \mid i = 0, \ldots, t; j = 1, \ldots, s_i\}$ es un sistema de generadores de $\mathfrak{a}$.
Dado $F = (b_0 + b_1 X + \cdots)X^h \in \mathfrak{a}$, tenemos $b_0 = \sum_{j=1}^{s_h} r_j a_{h,j}$, y por tanto $F - \sum_{j=1}^{s_h} r_j F_{h,j}$ se escribe en la forma $F'X^{h+1}$, siendo $F' \in A[[X]]$. De esta forma llegamos a una combinación $F - \sum r_{i,j} F_{i,j}$ que es de la forma $F'X^t \in \mathfrak{a}$.
Si $F = F'X^{t+k} \in \mathfrak{a}$, entonces como $\mathfrak{a}_t = \mathfrak{a}_{t+k}$, tenemos que $F - \sum_{j=1}^{s_t} r_{j,k} F_{t,j} X^k$ es una serie del tipo $F'X^{t+k+1}$, y existen coeficientes tales que $F - \sum_{j=1}^{s_t} r_{j,k} X^k F_{t,j} - \sum_{j=1}^{s_t} r_{j,k+1} X^{k+1} F_{t,j}$. Prosiguiendo de esta forma se tiene que F se escribe en la forma

$$F = \sum_{j=1}^{s_t} \left(\sum_{l=k}^{\infty} r_{j,l} X^l\right) F_{t,j}.$$

Por tanto $\{F_{i,j} \mid i = 0, \ldots, t; j = 1, \ldots, s_i\}$ es un sistema de generadores de $\mathfrak{a}$. □

Una demostración alternativa, consecuencia del Teorema (28.11.), es la siguiente:

DEMOSTRACIÓN. Se considera la aplicación $f : A[[X]] \longrightarrow A$ definida $f(\sum_{i=0}^{\infty} s_iX^i) = s_0$. Si $\mathfrak{p}$ es un ideal primo de $A[[X]]$, entonces $f(\mathfrak{p})$ es un ideal de A, y por tanto finitamente generado. Sea $f(\mathfrak{p}) = (a_1,\dots,a_t)$, y sean $h^{(1)},\dots,h^{(t)} \in \mathfrak{p}$ tales que $f(h^{(i)}) = a_i$, para $j = 1,\dots,t$.

Si $X \in \mathfrak{p}$, entonces $a_j = h^{(j)} - X\sum_{i=1}^{\infty} h_i^{(j)}X^{i-1} \in \mathfrak{p}$, y $X, a_1,\dots,a_t$ es un sistema de generadores de $\mathfrak{p}$.

Si $X \notin \mathfrak{p}$ vamos a ver que $h^{(1)},\dots,h^{(t)}$ es un sistema de generadores. Dado $s \in \mathfrak{p}$ existen $c_{0,j} \in A$ tales que $s_0 = \sum_{j=1}^{t} c_{0,j}a_j$, y por tanto $s - \sum_{j=1}^{t} c_{0,j}h^{(j)} = Xs^{(1)} \in \mathfrak{p}$. Como $\mathfrak{p}$ es primo y $X \notin \mathfrak{p}$ se verifica $s^{(1)} \in \mathfrak{p}$. Existen $c_{1,j} \in A$ tales que $s_0^{(1)} = \sum_{j=1}^{t} c_{1,j}a_j$, y por tanto $s^{(1)} - \sum_{j=1}^{t} c_{1,j}h^{(j)} = Xs^{(2)} \in \mathfrak{p}$, siendo $s^{(2)} \in \mathfrak{p}$. Observar que se tiene $s - \sum_{j=1}^{t}(c_{0,j} + c_{1,j}X)h^{(j)} = Xs^{(2)}$. Por inducción obtenemos una expresión del tipo

$$s - \sum_{j=1}^{t}(c_{0,j} + c_{1,j}X + \cdots + c_{r,j}X^r)h^{(j)} = Xs^{(r+1)} \in \mathfrak{p},$$

y por tanto tendremos $s = \sum_{j=1}^{t}(\sum_{i=0}^{\infty} c_{i,j}X^i)h^{(j)}$. Esto es, $\{h^{(1)},\dots,h^{(t)}\}$ es un sistema de generadores de $\mathfrak{p}$. Como cada ideal primo de $A[[X]]$ es finitamente generado, entonces $A[[X]]$ es un anillo noetheriano. □

Corolario. 28.13. (a la demostración. Kaplansky.)
Sea A un anillo y $\mathfrak{p} \subseteq A[[X]]$ un ideal primo del anillo de series formales de potencias. Son equivalentes:

(a) $\mathfrak{p}$ es finitamente generado.
(b) $\mathfrak{p}_0$ es finitamente generado.

En este caso si $\mathfrak{p}_0$ tiene un sistema de generadores formado por t elementos, entonces $\mathfrak{p}$ tiene un sistema formado por $t+1$ elementos, si $X \in \mathfrak{p}$, o por t elementos, si $X \notin \mathfrak{p}$.

Corolario. 28.14.
Sea A un anillo noetheriano y $X_1,\dots,X_n$ indeterminadas sobre A, entonces $A[[X_1,\dots,X_n]]$ es un anillo noetheriano.

Lema. 28.15.
Sea M un A–módulo noetheriano, entonces $A/\operatorname{Ann}_A(M)$ es un anillo noetheriano.
En particular si un anillo tiene un A–módulo fiel noetheriano, entonces es un anillo noetheriano.

DEMOSTRACIÓN. Llamamos $S = A/\operatorname{Ann}_A(M)$, entonces, considerando M como S–módulo tenemos que los retículos de A–submódulos y S–submódulos de M coinciden.

Podemos por tanto suponer que M es un A–módulo noetheriano y fiel. Para ver que A es un anillo noetheriano, supongamos que $M = m_1A + \cdots + m_rA$, entonces podemos definir un homomorfismo

$$f : A \to M^r, \qquad f(x) = (m_1x, \ldots, m_rx).$$

Si $f(x) = 0$, entonces $m_ix = 0$ para $1 \leq i \leq r$. Luego $x \in \operatorname{Ann}_A(M) = 0$, y por tanto f es un homomorfismo inyectivo. Como M^r es noetheriano, entonces A también lo es, ya que es isomorfo a un submódulo de M^r. □

Es bien conocido que si A es un anillo noetheriano, entonces $A[X]$ es también un anillo noetheriano. El recíproco también es cierto, ya que $A \cong A[X]/(X)$. También es fácil probar que si A es un anillo noetheriano, cada A–álgebra finitamente generada es también noetheriana, ya que es un cociente de un anillo de polinomios en un número finito de indeterminadas. Que el problema recíproco, que no resuelve el siguiente teorema.

Teorema. 28.16. (Teorema de Eakin–Nagata.)
Sea $B \supseteq A$ una A–álgebra, finitamente generada como A–módulo. Son equivalentes los siguientes enunciados:

(a) A es un anillo noetheriano.
(b) B es un anillo noetheriano.

DEMOSTRACIÓN. (b)⇒(a). Llamamos

$$\Gamma = \{\mathfrak{a}B \mid \mathfrak{a} \subseteq A,\ B/\mathfrak{a}B \text{ no es un } A\text{–módulo noetheriano}\}.$$

Si A no es noetheriano, entonces como $A \to B$, $x \mapsto 1x$, tenemos que B no es un A–módulo noetheriano, y por tanto $0 \in \Gamma$ y $\Gamma \neq \varnothing$. Utilizando que B es un anillo noetheriano, resulta que existe $\mathfrak{a}B \in \Gamma$ maximal.
Consideramos la extensión de anillos:

$$A' = A/\operatorname{Ann}_A(B/\mathfrak{a}B) \to B/\mathfrak{a}B = B',$$

entonces B' es un anillo noetheriano que es un A'–módulo finitamente generado, no es un A'–módulo noetheriano y cada cociente $B'/\mathfrak{b}B'$, con $\mathfrak{b} \subseteq A'$ es un A'–módulo noetheriano. Hacemos ahora el cambio $A \mapsto A'$ y $B \mapsto B'$.
Llamamos $\Lambda = \{X \mid X \text{ es un } A\text{–submódulo de } B \text{ y } \operatorname{Ann}_A(B/X) = 0\}$. Si $B = s_1A + \cdots + s_tA$, entonces los elementos de Λ pueden ser caracterizados por la propiedad:

$$\text{Para cada } 0 \neq a \in A,\ \{s_1a, \ldots, s_ta\} \nsubseteq X.$$

Ya que $0 \in \Lambda$, tenemos $\Lambda \neq \varnothing$. Sea $X_1 \subseteq X_2 \subseteq \cdots$ una cadena en Λ. Si llamamos $X = \cup X_n$ y si $X \notin \Lambda$, entonces existe $a \in A$ tal que $\{s_1a, \ldots, a_ta\} \subseteq X$, lo que es una contradicción. Tenemos pues que Λ es un conjunto inductivo.
Sea $X_0 \in \Lambda$ maximal, si B/X_0 es A–noetheriano, entonces $A/\operatorname{Ann}_A(B/X_0) = A$ es noetheriano ya que es un A–submódulo. Si B/X_0 no es A–noetheriano, entonces tenemos la siguiente situación: existe un A–módulo M que es un cociente de B y tal que:

(1) M no es noetheriano, es fiel y es finitamente generado.
(2) Para cada ideal $0 \neq \mathfrak{a} \subseteq A$ el cociente $M/M\mathfrak{a}$ es noetheriano.
(3) Para cada submódulo $0 \neq N \subseteq M$ el cociente M/N no es fiel

Sea $0 \neq N \subseteq M$, entonces M/N no es fiel y existe $a \in A \setminus \{0\}$ tal que $Ma \subseteq N$, entonces por (2), el cociente M/Ma es noetheriano y como consecuencia $N/Ma \subseteq M/Ma$ es finitamente generado. Además B era finitamente generado y por tanto M es finitamente generado y como consecuencia Ma es finitamente generado. Entonces N es finitamente generado. Tenemos que cada submódulo de M es finitamente generado, lo que implica que M es noetheriano. Esto es una contradicción. □

Anillos artinianos

La teoría dual a la de anillos noetherianos es la de los anillos artinianos. En este caso los resultados que se obtienen son más modestos, aunque, como más adelante veremos, cada anillo artiniano será un anillo noetheriano, e incluso podremos dar un teorema de estructura de los anillos artinianos.
Un anillo A se llama **artiniano** si A_A es un A–módulo artiniano.

Lema. 28.17.
Sea A un anillo, son equivalentes los siguientes enunciados:
(a) A es artiniano.
(b) Cada A–módulo finitamente generado es artiniano.

Lema. 28.18.
Si A es un anillo artiniano y si $\mathfrak{a}$ es un ideal, entonces $A/\mathfrak{a}$ es un anillo artiniano.

Módulos de longitud finita

Módulos artinianos no necesariamente son noetherianos, pero son de interés aquellos módulos que son simultáneamente artinianos y noetherianos. Estudiaremos estos módulos utilizando como herramienta esencial los módulos simples, por lo que comenzamos introduciendo este tipo particular de módulos.
Un A–módulo M se llama **simple** si es no nulo y sus únicos submódulos son 0 y M.

Lema. 28.19.
Sea M un A–módulo no nulo. Son equivalentes los siguientes enunciados:
(a) M es simple.
(b) Existe un ideal maximal $\mathfrak{a}$ de A tal que $M \cong A/\mathfrak{a}$.
(c) Cada elemento no nulo de M es un generador.

Proposición. 28.20. (Lema de Schur.)
Sea M un A–módulo simple, entonces tenemos que $\operatorname{End}_A(M)$ *es un anillo de división.*

Si M es un A–módulo, una **serie de submódulos** de M es una cadena estrictamente ascendente finita de submódulos

$$0 = M_0 \subset M_1 \subset \cdots \subset M_t = M.$$

Si se verifica que para cada índice i el cociente M_i/M_{i-1} es un A–módulo simple entonces se llama una **serie de composición** de M. En este caso los cocientes M_i/M_{i-1} se llaman **factores de composición** de M.

El número t se llama **longitud** de la serie de composición y los cocientes M_i/M_{i-1} se llaman **factores de composición**.

Vamos a probar que la longitud de una serie de composición de un A–módulo es un invariante.

Dos series de composición $0 = M_0 \subset M_1 \subset \cdots \subset M_t = M$ y $0 = N_0 \subset N_1 \subset \cdots \subset N_s = M$ son **equivalentes** si $t = s$ y existe una permutación $\sigma \in S_t$ tal que $M_i/M_{i-1} \cong N_{\sigma(i)}/N_{\sigma(i)-1}$, para cada $1 \leq i \leq t$.

Lema. 28.21.
Toda serie de submódulos de M que es equivalente a una serie de composición es una serie de composición.

Dada una serie de submódulos de M, por ejemplo

$$0 = M_0 \subset M_1 \subset \cdots \subset M_t = M,$$

un **refinamiento** es una serie de submódulos $0 = N_0 \subset N_1 \subset \cdots \subset N_s = M$ tal que para cada índice $1 \leq i \leq t$ existe un índice $1 \leq j_i \leq s$ tal que $M_i = N_{j_i}$.

Proposición. 28.22. (Teorema de Schreier.)
Cada dos series de submódulos de M tienen refinamientos equivalentes.

DEMOSTRACIÓN. Dadas dos series de submódulos

$$0 = M_0 \subset M_1 \subset \cdots \subset M_t = M, \text{ y} \tag{IV.1}$$

$$0 = N_0 \subset N_1 \subset \cdots \subset N_s = M, \tag{IV.2}$$

construimos un refinamiento de (IV.1) en la siguiente forma:

$$\begin{aligned}0 = M_1 \cap N_0 \subseteq M_1 \cap N_1 \subseteq \cdots \subseteq M_1 \cap N_s = M_1 \\ = M_1 + (M_2 \cap N_0) \subseteq \cdots \subseteq M_1 + (M_2 \cap N_s) = M_2 \\ = M_2 + (M_3 \cap N_0) \subseteq \cdots \subseteq M_{t-1} + (M_t \cap N_s) = M.\end{aligned} \qquad \text{(IV.3)}$$

Llamamos $M_{i,j} = M_{i-1} + (M_i \cap N_j)$, para $1 \leq i \leq t$ y $0 \leq j \leq s$. Observar que se tiene $M_{i-1,s} = M_{i,0}$. En la misma forma construimos un refinamiento para (IV.2).

$$\cdots \subseteq N_{j-1} + (N_j \cap M_i - 1) \subseteq N_{j-1} + (N_j \cap M_i) \subseteq \cdots \qquad \text{(IV.4)}$$

Veamos que (IV.3) y (IV.4) son equivalentes. En efecto, se tiene

$$\begin{aligned}\frac{M_{i,j}}{M_{i,j-1}} &= \frac{M_{i-1} + (M_i \cap N_j)}{M_{i-1} + (M_i \cap N_{j-1})} = \frac{M_{i-1} + (M_i \cap N_{j-1}) + (M_i \cap N_j)}{M_{i-1} + (M_i \cap N_{j-1})} \\ &\cong \frac{M_i \cap N_j}{(M_{i-1} + (M_i \cap N_{j-1})) \cap M_1 \cap N_j} = \frac{M_i \cap N_j}{M_i \cap (M_{i-1} + N_{j-1}) \cap M_1 \cap N_j} \\ &= \frac{M_i \cap N_j}{(M_{i-1} + N_{j-1}) \cap M_1 \cap N_j} = \frac{M_i \cap N_j}{(M_i \cap N_{j-1}) + (M_{i-1} \cap N_j)}.\end{aligned}$$

y en la misma forma

$$\frac{N_{j,i}}{N_{j,i-1}} \cong \frac{M_i \cap N_j}{(M_i \cap N_{j-1}) + (M_{i-1} \cap N_j)}.$$

□

Proposición. 28.23. (Teorema de Jordan–Hölder.)
Sea M un A–módulo que tiene una serie de composición de longitud t, entonces:

(1) Cada cadena estrictamente ascendente de submódulos de M se puede refinar a una serie de composición.
(2) Todas las series de composición de M tienen longitud t.

Si M es un A–módulo que tiene una serie de composición, llamamos **longitud** de M, y la representamos por $\operatorname{long}(M)$, a la longitud de sus series de composición. Como consecuencia diremos que M tiene **longitud finita** si tiene una serie de composición, y que tiene longitud infinita si no tiene una serie de composición.

Lema. 28.24.
Sea M un A–módulo. Son equivalentes:

(a) M tienen una serie de composición.
(b) M es noetheriano y artiniano.

Proposición. 28.25.
Sea $0 \to M' \to M \to M'' \to 0$ *una sucesión exacta corta de* A*–módulos. Son equivalentes los siguientes enunciados:*

(a) M *tiene longitud finita.*
(b) M' *y* M'' *tienen longitud finita.*

Además, la función $\operatorname{long}(-)$ *es aditiva sobre sucesiones exactas cortas de módulos de longitud finita, esto es,* $\operatorname{long}(M) = \operatorname{long}(M') + \operatorname{long}(M'')$ *si* M, M' *y* M'' *tienen longitud finita.*

29. Ejercicios

Módulos y homomorfismos de módulos

Ejercicio. 29.1.
Dado el $\mathbb{Z}$–módulo $X = \mathbb{Z}_2 \times \mathbb{Z}_2$.

(1) Determina todos los submódulos de X y dibuja el retículo de los submódulos de X.
(2) Encuentra tres submódulos de X, llámalos A, B, C, tales que:

$$(A+B)\cap C \neq (A\cap C)+(B\cap C), \qquad y \qquad (A\cap B)+C \neq (A+C)\cap(B+C).$$

esto es, el retículo de los submódulos no es necesariamente distributivo.
(3) Prueba que para cualquier módulo M y cualesquiera submódulos N, L, H, tales que $N \subseteq H$, se verifica

$$(N+L)\cap H = N+(L\cap H).$$

Esta última propiedad se llama la **ley modular** *y, como hemos comprobado, la verifican todos los módulos.*

SOLUCIÓN

Ejercicio. 29.2.
Se considera el $\mathbb{Z}$–módulo $Y = \mathbb{Z}_4 \times \mathbb{Z}_3$. Determina todos los submódulos de Y y dibuja el retículo de los submódulos de Y.

SOLUCIÓN

Ejercicio. 29.3.
Dado un submódulo N de un módulo M, siempre existe un submódulo de M maximal entre los que tienen intersección nula con N. Un submódulo de M que verifica esta propiedad se llama un ***pseudo–complemento*** *de N en M.*

(1) Prueba que si L es un pseudo–complemento de N en M, entonces $N+L$ es un submódulo de M que corta, de forma no trivial, a cada submódulo no nulo de M.
(2) Da un ejemplo de un módulo M y de un submódulo N de M que tenga al menos dos pseudo–complementos en M.

SOLUCIÓN

Ejercicio. 29.4.
Dado un módulo M, vamos a estudiar la unión de submódulos.

(1) *Si $\{M_i \mid i \in I\}$ es una cadena de submódulos, entonces $\cup_i M_i$ es un submódulo.*
(2) *Dados dos submódulos M_1 y M_2, se tiene que $M_1 \cup M_2$ es un submódulo si, y sólo si, $M_1 \subseteq M_2$ ó $M_2 \subseteq M_1$.*
(3) *Este resultado no se tiene para tres submódulos; estudiar el ejemplo que proporciona el grupo abeliano $\mathbb{Z}_2 \times \mathbb{Z}_2$.*
(4) *Sin embargo podemos generalizar a una familia finita de submódulos. Si $M_1, \ldots, M_t$ es una familia finita de submódulos tal que $\cup_{i=1}^t M_i$ es un submódulos, para cada $1 \leq s < t$ se tiene $\cap_{i=1}^s M_i \subseteq \cup_{j=s+1}^t M_j$ ó $\cap_{j=s+1}^t M_j \subseteq \cup_{i=1}^s M_i$.*

SOLUCIÓN

Módulos simples

Ejercicio. 29.5.
*Un A–módulo M se llama **simple** (o **irreducible**) si $M \neq 0$ y los únicos submódulos de M son M y 0.*

(1) *Demuestra que A es simple si, y sólo si, $M \neq 0$ y M es un módulo cíclico generado por cualquier elemento no nulo.*
(2) *Determina todos los $\mathbb{Z}$–módulos simples.*
(3) *Como A es conmutativo. Demuestra que M es simple si, y sólo si, es isomorfo (como A–módulo) a $A/\mathfrak{m}$, donde $\mathfrak{m}$ es un ideal maximal de A.*

SOLUCIÓN

Ejercicio. 29.6.
Sean M, N dos A–módulos simples.

(1) *Demuestra que todo homomorfismo no nulo $f : M \longrightarrow N$ es un isomorfismo.*
(2) *Deduce el **Lema de Schur**: Si M es simple, el anillo, no conmutativo, $\operatorname{End}_A(M)$ es un anillo de división.*

SOLUCIÓN

Ejercicio. 29.7.
Estudia los siguientes enunciados

(1) Considera el anillo $A = \mathbb{Z}_2 \times \mathbb{Z}_2$, y los ideales maximales $\mathfrak{m}_1 = \langle(1,0)\rangle$, $\mathfrak{m}_2 = \langle(0,1)\rangle$, $\mathfrak{m}_3 = \langle(1,1)\rangle$. ¿Es isomorfo $A/\mathfrak{m}_i$ isomorfo a $A/\mathfrak{m}_j$ si $i \neq j$?
(2) Prueba que para cada anillo A e ideales maximales $\mathfrak{m}_1, \mathfrak{m}_2$, se tiene $A/\mathfrak{m}_1 \cong A/\mathfrak{m}_2$ si, y sólo si, $\mathfrak{m}_1 = \mathfrak{m}_2$.

SOLUCIÓN

Hom

Ejercicio. 29.8.
Sean M_1, M_2, N A–módulos arbitrarios. Demuestra que existen isomorfismos (naturales) de A–módulos:

$$\begin{aligned}\mathrm{Hom}_A(M_1 \oplus M_2, N) &\cong \mathrm{Hom}_A(M_1, N) \oplus \mathrm{Hom}_A(M_2, N),\\ \mathrm{Hom}_A(N, M_1 \oplus M_2) &\cong \mathrm{Hom}_A(N, M_1) \oplus \mathrm{Hom}_A(N, M_2).\end{aligned}$$

Ver también los ejercicios (34.2.) y (34.3.). *SOLUCIÓN*

Ejercicio. 29.9.
Demuestra que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_d$, *donde* $d = \mathrm{m.c.d.}\{n, m\}$.
Ver también el ejercicio (34.5.). *SOLUCIÓN*

Ejercicio. 29.10.
Para un A–módulo M y una familia de A–módulos $\{M_i \mid i \in I\}$ existen isomorfismos

$$\begin{aligned}\mathrm{Hom}_A(\oplus_i M_i, M) &\cong \textstyle\prod_i \mathrm{Hom}_A(M_i, M),\\ \mathrm{Hom}_A(M, \textstyle\prod_i M_i) &\cong \textstyle\prod_i \mathrm{Hom}_A(M, M_i)\end{aligned}$$

Razona que estos isomorfismos son, respectivamente, consecuencia directa de la propiedad universal de la suma directa y el producto directo.

SOLUCIÓN

Módulos cocientes

Ejercicio. 29.11.
Utilizando el tercer teorema de isomorfía, determina todos los subgrupos y todos los posibles cocientes del grupo abeliano $\mathbb{Z}_n$.

SOLUCIÓN

Módulos libres

Ejercicio. 29.12.
Estudia los siguientes enunciados:

(1) Si $X, Y \in M_n(A)$ y $XY = I_n$, entonces $YX = I_n$.
(2) Si $X \in M_{n\times m}(A)$, $Y \in M_{m\times n}(A)$ y $XY = I_n$, entonces $n \leq m$.
(3) Si $X \in M_{n\times m}(A)$, $Y \in M_{m\times n}(A)$, $XY = I_n$ y $YX = I_m$, entoncesn $= m$.

SOLUCIÓN

Ejercicio. 29.13.
Utiliza el ejercicio (29.12.) para probar que si $A^n \cong A^m$, entonces $n = m$.

SOLUCIÓN

Ejercicio. 29.14.
Sea F un A–módulo y $F' \subseteq F$ un submódulo tal que F' y F/F' son móduloslibres. Demuestra que F es un módulo libre.

SOLUCIÓN

Ejercicio. 29.15.
Sea A un anillo, para cada epimorfismo $f : A^m \longrightarrow A^n$ se tiene $m \geq n$.

SOLUCIÓN

Ejercicio. 29.16.
Sea A un anillo, para cada monomorfismo $f : A^m \longrightarrow A^n$ se tiene $m \leq n$.

SOLUCIÓN

Ejercicio. 29.17.
Sea F un A–módulo libre de rango finito. Demuestra que existe un isomorfismo de A–módulos $\mathrm{Hom}_A(F,A) \cong F$.

SOLUCIÓN

Ejercicio. 29.18.
Sea F un A–módulo libre de rango n. Demuestra que para todo A–módulo M existe un isomorfismo de A–módulos $\mathrm{Hom}_A(F,M) \cong M^n$.

SOLUCIÓN

Módulos finitamente generados

Ejercicio. 29.19.
Sea N un A–submódulo de M y

(I) *N y M/N son finitamente generados;*
(II) *M es finitamente generado.*

Demuestra que (i)⇒(ii).
Da un ejemplo de que en general no se verifica (ii)⇒(i).

SOLUCIÓN

Ejercicio. 29.20.
Se considera un conjunto no vacío X y se define $A = \{f \mid f : X \to \mathbb{Q}\}$. Si en A se define la suma y el producto punto a punto y el elemento uno como la aplicación constante igual a 1, entonces A es un anillo conmutativo. Prueba:

(1) $g \in Af$ si, y sólo si, $f^{-1}(0) \subseteq g^{-1}(0)$.
(2) $h \in A(f,g)$ si, y sólo si, $f^{-1}(0) \cap g^{-1}(0) \subseteq h^{-1}(0)$.
(3) Todo ideal de A finitamente generado es un ideal principal.

SOLUCIÓN

Ejercicio. 29.21.
Prueba que todo módulo finitamente generado no nulo tiene un submódulo maximal.

SOLUCIÓN

Ejercicio. 29.22.
Sea A un dominio de integridad con cuerpo de fracciones K. Demuestra que K es un A-módulo finitamente generado si, y sólo si, $A = K$.
Ver también el Ejercicio (39.8.). SOLUCIÓN

Módulos noetherianos

Ejercicio. 29.23.
Sea M un A–módulo y $N_1, N_2 \subseteq M$ submódulos.

(1) Demuestra que si M/N_1 y M/N_2 son módulos noetherianos, también $M/(N_1 \cap N_2)$ esnoetheriano.
(2) Demuestra que si M/N_1 y M/N_2 son módulos artinianos, también $M/(N_1 \cap N_2)$ esartiniano.

SOLUCIÓN

Ejercicio. 29.24. (Lema de Fitting.)
Sea M un A–módulo noetheriano y $f : M \longrightarrow M$ un endomorfismo de A–módulos.

(1) Demuestra que existe un entero $n \geq 0$ tal que $\operatorname{Ker}(f^n) \cap \operatorname{Im}(f^n) = \{0\}$.
(2) Deduce que todo epimorfismo $f : M \longrightarrow M$ es un isomorfismo.

SOLUCIÓN

Módulos artinianos

Ejercicio. 29.25.
Estudia los siguientes enunciados:

(1) Para cada entero primo positivo p consideramos el conjunto $M = \{\frac{a}{p^t} \in \mathbb{Q} \mid a \in \mathbb{Z}, t \in \mathbb{N}\}$. Prueba que M es un submódulo $\mathbb{Q}$.

(2) *Llamamos P al grupo cociente $M/\mathbb{Z}$. Prueba que P contiene un subgrupo S_n isomorfo a $\mathbb{Z}_{p^n}$ para cada $n \in \mathbb{N}$, y que estos submódulo forman una cadena ascendente infinita $S_1 \subseteq S_2 \subseteq \cdots$ Como consecuencia P no es un grupo abeliano noetheriano.*
(3) *Prueba que todo subgrupo propio de P es igual a uno de los S_n.*
(4) *Prueba que P es un grupo abeliano artiniano.*

SOLUCIÓN

Anillos noetherianos

Ejercicio. 29.26.
Demuestra el recíproco del ***Teorema de la base de Hilbert****: Si el anillo de polinomios $A[X]$ es noetheriano, entonces A es noetheriano.*

SOLUCIÓN

Ejercicio. 29.27.
Sea A un dominio de ideales principales, demuestra que cada submódulo de un A–módulo libre finitamente generado es un módulo libre.
En particular cada subgrupo de $\mathbb{Z}^n$ es un grupo abeliano libre.

SOLUCIÓN

Ejercicio. 29.28.
Sea A un anillo noetheriano y $\mathfrak{a}$ un ideal propio de A. Prueba que existen ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ tales que $\mathfrak{a} \subseteq \mathfrak{p}_i$ para cada $i = 1, \ldots, t$ y $\mathfrak{p}_1 \cdots \mathfrak{p}_t \subseteq \mathfrak{a}$.

SOLUCIÓN

Ejercicio. 29.29.
Estudia los siguientes enunciados:

(1) *Sea A un anillo. Demuestra que para cada ideal propio $\mathfrak{a} \subseteq A$ existen ideales primos que son minimales sobre $\mathfrak{a}$.*
(2) *Sea A un anillo noetheriano. Demuestra que para cada ideal propio $\mathfrak{a} \subseteq A$ existe sólo un número finito de ideales primos minimales sobre $\mathfrak{a}$.*

(3) En este último caso, si $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ son los ideales primos minimales sobre un ideal $\mathfrak{a}$, existe $m \in \mathbb{N}$ tal que $(\mathfrak{p}_1 \cdots \mathfrak{p}_t)^m \subseteq \mathfrak{a}$.

SOLUCIÓN

Ejercicio. 29.30.
Ya conocemos que cada submódulo de un módulo libre finitamente generado sobre un dominio de ideales principales es un submódulo libre finitamente generado. Prueba el recíproco de este resultado; esto es, si cada submódulo de cada A–módulo libre finitamente generado es libre finitamente generado, entonces A es un dominio de ideales principales.

SOLUCIÓN

Ejercicio. 29.31.
Sea A un anillo. Prueba que si $\mathfrak{a} \subsetneq A$ es un ideal, maximal en el conjunto de los ideales que no son principales, entonces $\mathfrak{a}$ es un ideal primo.

SOLUCIÓN

Anillos no noetherianos

Ejercicio. 29.32.
Demuestra que los siguientes anillos no son noetherianos:

(1) El anillo de todas las funciones continuas $[0, 1] \longrightarrow \mathbb{R}$.
(2) El anillo de todas las aplicaciones $X \longrightarrow \mathbb{Z}_2$, donde X es unconjunto infinito.

SOLUCIÓN

Ejercicio. 29.33.
Sea K un cuerpo y X e Y indeterminadas. Demuestra que el subanillo

$$K[X, X^2Y, X^3Y^2, \ldots, X^iY^{i-1}, \ldots]$$

del anillo de polinomios $K[X, Y]$ no es noetheriano; lo que demuestra que los subanillos de anillos noetherianos no son necesariamente noetherianos y que subalgebras de álgebras finitamente generadas no son necesariamente finitamente generadas.

SOLUCIÓN

Ejercicio. 29.34.
Se considera el anillo $A = \mathbb{Z}^{\mathbb{N}}$. Prueba que A no es un anillo noetheriano.

SOLUCIÓN

Ejercicio. 29.35.
Se considera el anillo $A = \mathbb{Z}[X_1, \ldots, X_n, \ldots]/\mathfrak{a}$, siendo

$$\mathfrak{a} = (X_1 - X_i^{e_i} \mid i = 2, 3, \ldots).$$

(1) Prueba que si $e_i = 1$ para $i \geq 100$, entonces A es un anillo noetheriano.
(2) Prueba que en este caso A no es un $\mathbb{Z}$–módulo finitamente generado.
(3) Prueba que si $e_i = 1$ para i par y $e_i = 2$ para i impar mayor que 1, entonces A no es un anillo noetheriano

SOLUCIÓN

Ejercicio. 29.36.
Prueba que el anillo $\mathbb{Z} + X\mathbb{Q}[X]$ no es noetheriano.

SOLUCIÓN

Anillos artinianos

Ejercicio. 29.37.
Estudia los siguientes enunciados:
(1) Prueba que en un anillo artiniano A cada elemento que no es divisor de cero es invertible.
(2) Prueba que en un anillo artiniano A se tiene $\operatorname{Nil}(A) = J(A)$.
(3) Prueba que en un anillo artiniano todo ideal primo es maximal.

SOLUCIÓN

Ejercicio. 29.38.
Sabemos que todo anillo finito y toda álgebra de dimensión finita es artiniano y noetheriano. Vamos a estudiar algunos ejemplos anillos artinianos.

(1) Sea K un cuerpo y $F \in K[X]$ un polinomio no constante, el anillo $K[X]/(F)$ es un anillo artiniano, que es el producto directo finito de los anillos $K[X]/(F_i^{e_i})$, donde $F = F_1^{e_1} \cdots F_t^{e_t}$ es una descomposición de F en factores irreducibles.
(2) Sea K un cuerpo y $F \in K[X]$ un polinomio irreducible, entonces $K[X]/(F)$ es un anillo artiniano cuyos ideales propios forman una cadena y son de la forma $(F^j + (F^e))$, para $j = 1, \ldots, e$.
(3) Sea K un cuerpo y $A = K[X^2, X^3]/(X^4) = K[x^2, x^3]$; se tiene que A es un ideal artiniano con ideal maximal $\mathfrak{m} = (x^2, x^3)$, por tanto es un anillo local, y sus ideales no forman una cadena.

SOLUCIÓN

Ejercicio. 29.39.
Estudia los siguientes enunciados:

(1) Prueba que si M es un A–módulo noetheriano se tiene que $A/\operatorname{Ann}(M)$ es un anillo noetheriano.
(2) Da un ejemplo de que el mismo resultado no se verifica para un A–módulo artiniano.
(3) Prueba que el resultado es cierto para A–módulos artinianos finitamente generados.

SOLUCIÓN

Ejercicio. 29.40.
En un anillo A un elemento $0 \neq a \in A$ se llama ***minimal*** *si $\operatorname{Ann}(a)$ es un ideal maximal.*

(1) Prueba que en un anillo artiniano cada ideal no nulo contiene un elemento minimal.
(2) Prueba que en un anillo artiniano para cada ideal propio $\mathfrak{a}$ existe un elemento $a \in A$ tal que $(\mathfrak{a} : a)$ es un ideal maximal.
(3) (Lema de Nakayama para anillos artinianos).Prueba que en un anillo artiniano para cada ideal no nulo $\mathfrak{a} \subseteq A$ se tiene $\mathfrak{a}J \subsetneqq \mathfrak{a}$, donde $J = J(A)$ es el radical de Jacobson.
(4) Prueba que en un anillo artiniano el radical de Jacobson es un ideal nilpotente.

SOLUCIÓN

Ejercicio. 29.41.
Si A es un anillo artiniano local con ideal maximal $\mathfrak{m}$. Como $\mathfrak{m}$ es un ideal nilpotente, existe $n \in \mathbb{N}$ tal que $\mathfrak{m}^n = 0$. Tenemos por tanto una cadena de submódulos $A \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^n = 0$. Cada factor $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ es un $A/\mathfrak{m}$–módulo, pero no podemos asegurar que A sea un $A/\mathfrak{m}$–módulo.Tenemos como consecuencia que cada anillo local artiniano es en cierto modo un anillo finito (con respecto al cuerpo residual).

(1) Estudiar el caso de $A = \mathbb{Z}_4$ con ideal maximal $2\mathbb{Z}_4$ y cuerpo residual $\mathbb{Z}_2$. Es claro que $\mathbb{Z}_4$ no es un $\mathbb{Z}_2$–módulo

(2) Hay otros casos en los que A tiene estructura de $A/\mathfrak{m}$–módulo, pero esta estructura no es compatible con la multiplicación en A.Se considera $A = \mathbb{K}[X]/(F^e)$, siendo $F \in K[X]$ un polinomio irreducible.

SOLUCIÓN

Módulos de longitud finita

Ejercicio. 29.42.
Sean $N, H \subseteq M$ submódulos de un A–módulo M. Prueba que

$$\operatorname{long}(N) + \operatorname{long}(H) = \operatorname{long}(N + H) + \operatorname{long}(N \cap H).$$

SOLUCIÓN

Ejercicio. 29.43.
Sea $0 \to M_1 \to M_2 \to \cdots \to M_n \to 0$ una sucesión exacta de A–módulos, con $\operatorname{long}(M_i)$ finito para cada índice $i = 1, 2, \ldots, n$. Prueba que

$$\sum_{i=1}^{n} (-1)^i \operatorname{long}(M_i) = 0.$$

SOLUCIÓN

Ejercicio. 29.44.
Prueba que para cada A–módulo M se tiene

$$\operatorname{long}(M) = \sup\{\operatorname{long}(N) \mid N \subseteq M \text{ finitamente generado}\}.$$

SOLUCIÓN

Ejercicio. 29.45.
Sea M un A–módulo, y $a \in A$ un elemento tal que si $am = 0$, entonces $m = 0$, para cada $m \in M$. Prueba:

(1) $aM = \{am \mid m \in M\}$ *es un submódulo de* M *isomorfo a* M.
(2) *Para cada submódulo* $N \subseteq M$ *se tiene* $M/N \cong aM/aN$.
(3) *Para cada entero positivo* n *se tiene* $\operatorname{long}(M/a^nM) = n \operatorname{long}(M/aM)$.

SOLUCIÓN

Anillos de series formales de potencias

Ejercicio. 29.46.
Sea A *un anillo noetheriano y* $F = \sum_{i=0}^{\infty} a_i X^i \in A[[X]]$ *una serie formal de potencias. Definimos el* ***contenido*** *de* F *como el ideal* $c(F) = (a_0, a_1, \ldots) \subseteq A$. *Prueba que son equivalentes:*

(a) F *es nilpotente.*
(b) *Todos los coeficientes de* F *son nilpotentes.*
(c) *Existe* $n \in \mathbb{N}$ *tal que* $a_i^n = 0$ *para cada índice* i.

SOLUCIÓN

Capítulo V

Categorías y funtores

Introducción[1]

La teoría de categorías se introduce con el fin de unificar diversas construcciones sobre varias estructuras, y también para crear nuevos objetos que nos permitan estudiar y clasificar estas estructuras. Éste es el caso de la categoría de módulos sobre un anillo, que permite estudiar el anillo a través de las propiedades de esta categoría y de sus objetos.

En este capítulo vamos a hacer una introducción elemental a la teoría de categorías y funtores; haremos especial hincapié en los ejemplos y en las construcciones universales (funtores adjuntos). Finalizamos el capítulo introduciendo los funtores Hom y producto tensor y las sucesiones exactas.

[1]Este capítulo es opcional.

30. Categorías y funtores

Categorías

Esta es una introducción intuitiva a la Teoría de Categorías y Funtores. Partimos de la noción de clase. Una **clase** es un objeto matemático que es definido por las propiedades que verifican los elementos que lo forman. Si C es elemento de una clase $\mathcal{C}$ escribimos: $C \in \mathcal{C}$.

Dadas dos clases $\mathcal{C}$ y $\mathcal{D}$, una **aplicación** f de $\mathcal{C}$ a $\mathcal{D}$ es una regla que asocia a cada elemento de $\mathcal{C}$ un elemento de $\mathcal{D}$, escribimos $f : \mathcal{C} \longrightarrow \mathcal{D}$. La aplicación f se llama **biyectiva** si existe una aplicación $g : \mathcal{D} \longrightarrow \mathcal{C}$ tal que $f \circ g$ y $g \circ f$ son la identidad en $\mathcal{D}$ y $\mathcal{C}$, respectivamente.

El producto cartesiano de dos clases es otra clase.

Un **conjunto** es un elemento de la clase $\mathcal{S}$ de todos los conjuntos, los grupos son los elementos de la clase $\mathcal{G}$ de todos los grupos, etc. Existe una aplicación de $\mathcal{G}$ a $\mathcal{S}$ que asocia a cada grupo el conjunto subyacente sobre el que está definido. Amén de los señalados existen más ejemplos de clases: por ejemplo, cada conjunto va a ser una clase.

Una **categoría** $\mathcal{C}$ es un par formado por dos clases: $\mathcal{O}\mathrm{b}(\mathcal{C})$, la clase de objetos, y $\mathcal{M}\mathrm{or}(\mathcal{C})$, la clase morfismos, que verifica:

(I) $\mathcal{M}\mathrm{or}(\mathcal{C})$ es una clase de conjuntos disjuntos dos a dos.
(II) Existe una aplicación biyectiva $\mathrm{Hom}_{\mathcal{C}} : \mathcal{O}\mathrm{b}(\mathcal{C}) \times \mathcal{O}\mathrm{b}(\mathcal{C}) \to \mathcal{M}\mathrm{or}(\mathcal{C})$.
(III) Para cada terna A, B, $C \in \mathcal{O}\mathrm{b}(\mathcal{C})$ existe una aplicación $\circ$, definida:

$$\circ : \mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C); \quad (f, g) \mapsto f \circ g$$

$f \circ g$ se llama la **composición** de f y g.
(IV) Propiedad asociativa de la composición. Se verifica $(f \circ g) \circ h = f \circ (g \circ h)$ para cada $f \in \mathrm{Hom}_{\mathcal{C}}(C, D)$, $g \in \mathrm{Hom}_{\mathcal{C}}(B, C)$, $h \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, $A, B, C, D \in \mathcal{O}\mathrm{b}(\mathcal{C})$.
(V) Existencia de identidades. Para cada $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ existe $\mathrm{id}_A \in \mathrm{Hom}_{\mathcal{C}}(A, A)$ tal que $\mathrm{id}_A \circ f = f$ y $g \circ \mathrm{id}_A = g$ para cada $f \in \mathrm{Hom}_{\mathcal{C}}(B, A)$ y $g \in \mathrm{Hom}_{\mathcal{C}}(A, C)$, B, $C \in \mathcal{O}\mathrm{b}(\mathcal{C})$.

Tenemos en primer lugar las siguientes propiedades y definiciones:

(1) Para cada $A \in \mathcal{O}\mathrm{b}(\mathcal{C})$ existe un único elemento id_A verificando la propiedad (v). El elemento id_A se llama la **identidad** de A.
(2) Si $f \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, entonces podemos notarlo $f : A \to B$ ó $A \xrightarrow{f} B$; A se llama el **dominio** de f y B se llama el **codominio**.
(3) Una categoría $\mathcal{C}$ se llama **pequeña** si $\mathcal{O}\mathrm{b}(\mathcal{C})$ es un conjunto.
(4) Dada una categoría $\mathcal{C}$ llamamos **morfismos** de $\mathcal{C}$ a los elementos de los conjuntos de $\mathcal{M}\mathrm{or}(\mathcal{C})$.
(5) Una categoría $\mathcal{C}$ se llama **discreta** si todos sus morfismos son identidades, y se llama **conexa** si para cada par de objetos A y B se tiene que $\mathrm{Hom}_{\mathcal{C}}(A, B)$ es no vacío.

Ejemplo. 30.1.
La categoría de conjuntos y aplicaciones se representa por $\mathcal{S}et$ y tiene por clase de objetos la clase de todos los conjuntos, y para cada dos conjuntos A y B el conjunto $\mathrm{Hom}_{\mathcal{S}et}(A, B)$ está formado por todas las aplicaciones de A en B; la composición es la composición usual de aplicaciones.

Ejemplo. 30.2.
La categoría $\mathcal{C}$ de conjuntos y relaciones; la clase de objetos es la clase de todos los conjuntos y para cada dos conjuntos A y B el conjunto $\operatorname{Hom}_{\mathcal{C}}(A,B)$ está formado por todas las relaciones de A a B. La composición es la composición de relaciones.

Ejemplo. 30.3.
Para cada anillo (resp. monoide) no necesariamente conmutativo R podemos definir una categoría $\mathcal{R}$ cuya clase de objetos contiene únicamente a R y $\operatorname{Hom}_{\mathcal{R}}(R,R) = R$, con la composición definida como la multiplicación.

Ejemplo. 30.4.
Si X es un conjunto con una relación de preorden $\leq$, (verifica las propiedades reflexiva y transitiva), podemos definir una categoría $\mathcal{X}$ cuya clase de objetos es el conjunto X y para $x_1,\ x_2 \in X$ si $x_1 \leq x_2$ tomamos $\operatorname{Hom}_{\mathcal{X}}(x_1,x_2)$ como un conjunto unitario, y si $x_1 \nleq x_2$, entonces $\operatorname{Hom}_{\mathcal{X}}(x_1,x_2)$ es vacío. La composición se define de la forma obvia.

Ejemplo. 30.5.
Sea R un anillo, definimos una categoría $\mathcal{C}$ cuyos objetos son los números enteros positivos y para dos objetos n y m definimos $\operatorname{Hom}_{\mathcal{C}}(n,m)$ como el conjunto de las matrices $m \times n$ con coeficientes en R. La composición es la multiplicación de matrices.

Ejemplo. 30.6.
Otros ejemplos de categorías son los siguientes:

(1) La categoría de conjuntos con aplicaciones inyectivas, resp. sobreyectivas.
(2) La categoría de semigrupos y homomorfismos de semigrupos $\mathcal{S}gr$.
(3) La categoría de monoides y homomorfismos de monoides, $\mathcal{M}on$.
(4) La categoría de grupos y homomorfismos de grupos, $\mathcal{G}r$.
(5) La categoría de grupos abelianos y homomorfismos de grupos, $\mathcal{A}b$.
(6) Para cada anillo R la categoría de R–módulos a izquierda y homomorfismos de R–módulos, R–***Mod***.
(7) La categoría de anillos y homomorfismos de anillos, $\mathcal{R}ing$.
(8) La categoría de retículos y homomorfismos de retículos, $\mathcal{L}at$.
(9) La categoría de conjuntos con un punto distinguido y aplicaciones que respetan el punto, $p\mathcal{S}et$.
(10) La categoría de dominios de integridad y homomorfismos de anillos inyectivos, $\mathcal{D}om\mathcal{I}nt$.
(11) La categoría de cuerpos, $\mathcal{F}ield$.

Ejemplo. 30.7.
Es posible también construir categorías a partir de otras dadas. Veamos el siguiente ejemplo.

Dada una categoría $\mathcal{C}$ consideramos una nueva categoría, a la que representaremos por $\mathcal{C}(2)$, cuyos objetos son las ternas (A,f,B), donde A y B son objetos de $\mathcal{C}$ y donde $f \in \operatorname{Hom}_{\mathcal{C}}(A,B)$. Un morfismo entre dos objetos (A_1,f_1,B_1) y (A_2,f_2,B_2) es un par (g,h), donde $g \in \operatorname{Hom}_{\mathcal{C}}(A_1,A_2)$, $h \in \operatorname{Hom}_{\mathcal{C}}(B_1,B_2)$ y $h \circ f_1 = f_2 \circ g$, esto es, el siguiente diagrama es conmutativo.

$$\begin{array}{ccc} A_1 & \xrightarrow{f_1} & B_1 \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ A_2 & \xrightarrow{f_2} & B_2 \end{array}$$

Otra construcción del mismo tipo es la siguiente:

Ejemplo. 30.8.
Sean $\mathcal{C}_1, \ldots, \mathcal{C}_r$ categorías, definimos una nueva categoría, llamada **categoría producto**, a la que representaremos por $\mathcal{C}_1 \times \cdots \times \mathcal{C}_r$, y cuyos objetos son r–uplas $(A_1, \ldots, A_r)$, con $A_i \in \mathcal{O}\mathrm{b}(\mathcal{C}_i)$, $i = 1, \ldots, r$ y cuyos morfismos están dados por la siguiente relación:

$$\mathrm{Hom}_{\mathcal{C}_1 \times \cdots \times \mathcal{C}_r}((A_1, \ldots, A_r), (B_1, \ldots, B_r)) = \mathrm{Hom}_{\mathcal{C}_1}(A_1, B_1) \times \cdots \times \mathrm{Hom}_{\mathcal{C}_r}(A_r, B_r),$$

siendo la composición componente a componente.

Si $\mathcal{C}$ es una categoría, llamamos **subcategoría** de $\mathcal{C}$ a una categoría $\mathcal{D}$ que verifique:

(I) $\mathcal{O}\mathrm{b}(\mathcal{D}) \subseteq \mathcal{O}\mathrm{b}(\mathcal{C})$.
(II) $\mathrm{Hom}_{\mathcal{D}}(A, B) \subseteq \mathrm{Hom}_{\mathcal{C}}(A, B)$, si $A, B \in \mathcal{O}\mathrm{b}(\mathcal{D})$.
(III) La identidad de $A \in \mathcal{O}\mathrm{b}(\mathcal{D})$ es la misma que en $\mathcal{C}$.
(IV) La composición en $\mathcal{D}$ es igual que en $\mathcal{C}$.

Una subcategoría $\mathcal{D}$ de una categoría $\mathcal{C}$ es llama **plena** si para cada par de objetos $A, B \in \mathcal{O}\mathrm{b}(\mathcal{D})$ se tiene $\mathrm{Hom}_{\mathcal{D}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(A, B)$.

Ejemplos. 30.9.
(1) La categoría de grupos finitos es una subcategoría plena de la categoría de grupos.
(2) La categoría de monoides es una subcategoría de la categoría de semigrupos y no es una subcategoría plena, (un homomorfismo de semigrupos no tiene por qué mantener la unidad, si ésta existe).
(3) La categoría de grupos no es una subcategoría de la categoría de conjuntos.
(4) Para cada anillo R la categoría de los R–módulos izquierda finitamente generados es una subcategoría plena de la categoría de R–módulos.

Veamos un concepto que está íntimamente ligado a la noción de categoría, el concepto de **dualidad**. Si $\mathcal{C}$ es una categoría, definimos la **categoría opuesta**, $\mathcal{C}^{op}$, de $\mathcal{C}$, mediante:

(I) $\mathcal{O}\mathrm{b}(\mathcal{C}^{op}) = \mathcal{O}\mathrm{b}(\mathcal{C})$.
(II) $\mathrm{Hom}_{\mathcal{C}^{op}}(A, B) = \mathrm{Hom}_{\mathcal{C}}(B, A)$, para cada $A, B \in \mathcal{O}\mathrm{b}(\mathcal{C})$.
(III) La composición $\star$ en $\mathcal{C}^{op}$ es $f \star g = g \circ f$, para $f \in \mathrm{Hom}_{\mathcal{C}^{op}}(B, C)$ y $g \in \mathrm{Hom}_{\mathcal{C}^{op}}(A, B)$.

Intuitivamente la categoría $\mathcal{C}^{op}$ se obtiene a partir de la categoría $\mathcal{C}$ invirtiendo todos sus morfismos. Es claro que $\mathcal{C}^{op}$ es una categoría y que $(\mathcal{C}^{op})^{op} = \mathcal{C}$.

Principio de dualidad

Si $\mathcal{P}$ es una propiedad de categorías (una propiedad entre objetos y morfismos) y si estudiamos esta propiedad en $\mathcal{C}^{op}$ y la pasamos luego a $\mathcal{C}$, entonces obtenemos una nueva propiedad en $\mathcal{C}$, a la que llamaremos **propiedad dual de** $\mathcal{P}$ y la representaremos por $\mathcal{P}^\star$.

Ejemplo. 30.10.
En la categoría de R–módulos izquierda un homomorfismo $f : M \longrightarrow M'$ que es simplificable a izquierda se llama un **monomorfismo**, esto es, si $f \circ g = f \circ h$ implica que $g = h$ para cualesquiera $g, h : N \longrightarrow M$. La noción dual es la de **epimorfismo** u homomorfismo simplificable a derecha.

En la categoría $\mathcal{S}et$ tenemos los siguientes resultados:

Resultado:
Para una aplicación $f : A \longrightarrow B$ entre conjuntos son equivalentes las siguientes propiedades:
(a) f es un monomorfismo.
(b) f es invertible a izquierda. (Existe $g : B \longrightarrow A$ tal que $g \circ f = id_A$.)

El resultado dual es:

Resultado dual:
Para una aplicación $f : A \longrightarrow B$ entre conjuntos son equivalentes las siguientes propiedades:
(a) f es un epimorfismo.
(b) f es invertible a derecha. (Existe $g : B \longrightarrow A$ tal que $f \circ g = id_B$.)

Al estudiar estos mismos resultados en otras categoría podemos observar que no son ciertos; por ejemplo un monomorfismo en la categoría de A–módulos no es necesariamente invertible a izquierda. Considerar el ejemplo $2\mathbb{Z} \longrightarrow \mathbb{Z}$. Y lo mismo ocurre para los epimorfismos. Podemos enunciar sin embargo resultados parecidos:

Resultado:
Para una homomorfismo $f : M \longrightarrow N$ entre A–módulos son equivalentes las siguientes propiedades:
(a) f es un monomorfismo.
(b) $\mathrm{Ker}(f) = 0$.

El resultado dual es:

Resultado dual:
Para una homomorfismo $f : M \longrightarrow N$ entre A–módulos son equivalentes las siguientes propiedades:
(a) f es un epimorfismo.
(b) $\mathrm{Coker}(f) = 0$, o equivalentemente $\mathrm{Im}(f) = N$.

Observa que al tener elementos los objetos de la categoría de módulos, los conceptos de monomorfismo y epimorfismo se identifican con los de aplicación inyectiva (= monomorfismo en la categoría de conjuntos) y sobreyectiva (= epimorfismo en la categoría de conjuntos); pudiendo extender los resultados anteriores con la propiedad adicional de ser inyectiva o sobreyectiva según el caso. (¡Es de destacar que

los conceptos de inyectivo o sobreyectivo no son conceptos definidos en la categoría de módulos, sino que necesitamos hacer uso de conceptos ajenos a la misma como el de elemento de sus objetos!)
Veamos que una propiedad puede ser cierta en una categoría mientras que la propiedad dual puede ser falsa.
Si consideramos ahora la categoría de anillos, a la que hemos representado por $\mathcal{R}ing$, en ella tenemos:

Resultado:
Para un homomorfismo de anillos $f : A \longrightarrow A$ en $\mathcal{R}ing$ son equivalentes las siguientes propiedades:
(a) f es un monomorfismo.
(b) f es una aplicación inyectiva.

Para la demostración de este hecho remitimos a los ejercicios.
El resultado dual sería:

Resultado dual:
Para un homomorfismo de anillos $f : A \longrightarrow B$ en la categoría $\mathcal{R}ing$ son equivalentes las siguientes propiedades:
(a) f es un epimorfismo.
(b) f es una aplicación sobreyectiva.

Este resultado no es cierto como prueba el siguiente ejemplo:
La inclusión $\mathbb{Z} \longrightarrow \mathbb{Q}$ es un epimorfismo en la categoría de anillos, y no es una aplicación sobreyectiva.

Una propiedad $\mathcal{P}$ se llama **autodual** si $\mathcal{P} = \mathcal{P}^\star$.

Ejemplo. 30.11.
En la categoría de A–módulos un A–módulo S es **simple** si no tiene submódulos propios no triviales. La noción dual se aplicaría a los módulos que no tienen cocientes propios no triviales. Por lo tanto el concepto de objeto simple en la categoría A–***Mod*** es un concepto autodual.
Si consideramos la categoría de grupos, $\mathcal{G}r$, tenemos dos nociones de objeto simple:
Simple-1: grupos que no tienen subgrupos propios no triviales.
Simple-1*: grupos que no tienen cocientes propios no triviales.
El grupo alternado A_5 es un grupo simple-1*, ya que no tiene subgrupos normales propios, pero no es un grupo simple-1, ya que sí tiene subgrupos propios no triviales. Por lo tanto la noción “simple"no es un concepto autodual en la categoría $\mathcal{G}r$.
En la categoría de grupos el concepto de **grupo simple** es el que aquí hemos tratado como grupo simple-1*.

Una propiedad $\mathcal{P}$ es cierta en una categoría $\mathcal{C}$ si, y sólo si, la propiedad $\mathcal{P}^\star$ es cierta en la categoría $\mathcal{C}^{op}$.
Como consecuencia, si una propiedad $\mathcal{P}$ es cierta en *todas* las categorías, también en todas las categorías lo es su propiedad dual $\mathcal{P}^\star$.

Funtores

Si $\mathcal{C}$ y $\mathcal{D}$ son dos categorías, un **funtor** de $\mathcal{C}$ a $\mathcal{D}$ se define como un par de funciones (F_o, F_m) verificando:

(I) $F_o : \mathcal{O}b(\mathcal{C}) \to \mathcal{O}b(\mathcal{D})$.
(II) $F_{m,A,B} : \mathrm{Hom}_{\mathcal{C}}(A,B) \to \mathrm{Hom}_{\mathcal{D}}(F_o(A), F_o(B))$.
(III) $F_{m,A,A}(\mathrm{id}_A) = \mathrm{id}_{F_o(A)}$.
(IV) Si $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$ y $g \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ son morfismos de $\mathcal{C}$, entonces

$$F_{m,A,C}(g \circ f) = F_{m,B,C}(f) \circ F_{m,A,B}(g).$$

Para simplificar llamamos simplemente $F_o(A) = F(A)$ y $F_{m,A,B}(f) = F(f)$, por lo tanto

(1) Para cada objeto A de $\mathcal{C}$ tenemos que $F(A)$ un objeto de $\mathcal{D}$.
(2) Para cada homomorfismo $f : A \longrightarrow B$ en $\mathcal{C}$ tenemos un homomorfismo $F(f) : F(A) \longrightarrow F(B)$ en $\mathcal{D}$.
(3) $F(\mathrm{id}_A) = \mathrm{id}_{F(A)}$.
(4) Si $A \xrightarrow{f} B \xrightarrow{g} C$ se tiene $F(g \circ f) = F(g) \circ F(f)$.

Si F es un funtor de $\mathcal{C}$ a $\mathcal{D}$ lo representamos por $F : \mathcal{C} \to \mathcal{D}$. Llamamos **dominio** de F a $\mathcal{C}$ y **codominio** de F a $\mathcal{D}$.

Ejemplos. 30.12.

(1) Para cada categoría $\mathcal{C}$ tenemos un funtor $\mathrm{id}_{\mathcal{C}}$ de $\mathcal{C}$ a $\mathcal{C}$ llamado **funtor identidad** que está definido por $\mathrm{id}_{\mathcal{C}}(A) = A$ para cada objeto A y $\mathrm{id}_{\mathcal{C}}(f) = f$ para cada morfismo f.
(2) Si $\mathcal{D}$ es una subcategoría de una categoría $\mathcal{C}$, existe un funtor de $\mathcal{D}$ a $\mathcal{C}$ llamado **funtor inclusión** definido de la forma obvia.
(3) El funtor abelianización en grupos asocia a cada grupo G el grupo cociente $G/[G,G]$, y a cada morfismo de grupos $f : G \to G'$ el morfismo inducido $\overline{f} : G/[G,G] \to G'/[G',G']$.
(4) Una categoría $\mathcal{C}$ se llama **concreta** si cada objeto tiene asociado un conjunto en el siguiente sentido: existe un funtor $U : \mathcal{C} \to \mathcal{S}et$ que es inyectivo sobre morfismos, esto es, $U : \mathrm{Hom}_{\mathcal{C}}(A,B) \to \mathrm{Hom}_{\mathcal{S}et}(U(A), U(B))$ es inyectiva para cada par $A, B \in \mathcal{O}b(\mathcal{C})$.
(5) Funtor libre en grupos, semigrupos, monoides y módulos; estos funtores tiene como dominio la categoría de conjuntos.

Lema. 30.13.
Si $F : \mathcal{C} \to \mathcal{D}$ y $G : \mathcal{D} \to \mathcal{E}$ son funtores, entonces existe un nuevo funtor $G \circ F : \mathcal{C} \to \mathcal{E}$ definido por:

Para cada objeto A de $\mathcal{C}$, $(G \circ F)(A) = G(F(A))$;

Para cada $f \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, $(G \circ F)(f) = G(F(f))$.

El funtor $G \circ F$ se llama **composición** de F y G y lo representamos también simplemente por GF.

Definimos un **funtor contravariante** entre las categorías $\mathcal{C}$ y $\mathcal{D}$ como un funtor $F : \mathcal{C}^{op} \to \mathcal{D}$, ó equivalentemente como un funtor $F^{op} : \mathcal{C} \to \mathcal{D}^{op}$.

Ejemplo. 30.14.
Para cada funtor $F : \mathcal{C} \to \mathcal{D}$ existe un funtor contravariante $F' : \mathcal{C}^{op} \to \mathcal{D}$ definido por $F'(A) = F(A)$ y $F'(f) = F(f)$ para objetos y morfismos respectivamente.

Llamamos **bifuntor** a un funtor cuyo dominio es una categoría producto $\mathcal{C}_1 \times \mathcal{C}_2$.

Teorema. 30.15.
Si $F : \mathcal{C}_1 \times \mathcal{C}_2 \to \mathcal{D}$ es un bifuntor, entonces:
(1) Para cada $A \in \mathcal{O}\mathrm{b}(\mathcal{C}_1)$ existe un funtor asociado $F(A,-) : \mathcal{C}_2 \to \mathcal{D}$, definido por $F(A,-)(B) = F(A,B)$ y $F(A,-)(f) = F(\mathrm{id}_A, f)$ para objetos y morfismos respectivamente.
(2) Para cada $B \in \mathcal{O}\mathrm{b}(\mathcal{C}_2)$ existe un funtor asociado $F(-,B) : \mathcal{C}_1 \to \mathcal{D}$, definido por $F(-,B)(A) = F(A,B)$ y $F(-,B)(f) = F(f, \mathrm{id}_B)$ para objetos y morfismos respectivamente.

Ejemplo. 30.16.
Sea $\mathcal{C}$ una categoría, definimos un bifuntor

$$\mathrm{Hom}_{\mathcal{C}} : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{S}et$$

mediante: Para objetos en la forma obvia, y si $f_i : A_i \to B_i$ son morfismos de $\mathcal{C}$, entonces

$$\mathrm{Hom}_{\mathcal{C}}(f_1, f_2) : \mathrm{Hom}_{\mathcal{C}}(B_1, A_2) \to \mathrm{Hom}_{\mathcal{C}}(A_1, B_2)$$

definido por:

$$\mathrm{Hom}_{\mathcal{C}}(f_1, f_2)(h) = f_2 h f_1 (= f_1^*(f_2)_*(h)),$$

para cada $h \in \mathrm{Hom}_{\mathcal{C}}(B_1, A_2)$.

$$\begin{array}{ccc} A_1 & \xrightarrow{\mathrm{Hom}_{\mathcal{C}}(f_1,f_2)(h)} & B_2 \\ {\scriptstyle f_1}\downarrow & & \uparrow{\scriptstyle f_2} \\ B_1 & \xrightarrow{\quad h \quad} & A_2 \end{array}$$

Llamamos a $\mathrm{Hom}_{\mathcal{C}}$ el **funtor Hom valorado en conjuntos**. Para cada objeto A de $\mathcal{C}$ llamamos a $\mathrm{Hom}_{\mathcal{C}}(A,-)$ el **funtor Hom covariante** de $\mathcal{C}$ respecto a A, y a $\mathrm{Hom}_{\mathcal{C}}(-,A)$ el **funtor Hom contravariante** de $\mathcal{C}$ respecto a A. En general tratamos el funtor $\mathrm{Hom}_{\mathcal{C}}$ de $\mathcal{C} \times \mathcal{C}$ a $\mathcal{S}et$.

Observación. 30.17.
No se puede hablar de la categoría de categorías y funtores, ya que los objetos no formarían una clase, pero podemos formalmente extender la noción de categoría, obteniendo un nuevo concepto, el de **quasicategoría** para, de esta forma, poder estudiar categorías y funtores como si fuesen objetos y morfismos de una quasicategoría.

Apéndice

Si $\mathcal{C}$ es una categoría, una relación de equivalencia entre morfismos de $\mathcal{C}$ es una relación de equivalencia $\sim$ en cada conjunto $\mathrm{Hom}_{\mathcal{C}}(A,B)$ verificando: si $f_1 \sim f_2$ para $f_1, f_2 \in \mathrm{Hom}_{\mathcal{C}}(B,C)$ y $g_1 \sim g_2$ para $g_1, g_2 \in \mathrm{Hom}_{\mathcal{C}}(A,B)$, entonces $f_1 \circ g_1 \sim f_2 \circ g_2$ en $\mathrm{Hom}_{\mathcal{C}}(A,C)$.

Lema. 30.18.
Si $\mathcal{C}$ es una categoría y $\sim$ es una relación de equivalencia entre morfismos de $\mathcal{C}$, entonces la categoría $\widetilde{\mathcal{C}}$, definida por $\mathcal{O}\mathrm{b}(\widetilde{\mathcal{C}}) = \mathcal{O}\mathrm{b}(\mathcal{C})$ y

$$\mathrm{Hom}_{\widetilde{\mathcal{C}}} = \mathrm{Hom}_{\mathcal{C}}(A,B)/\sim, \text{ para todos } A,B \in \mathcal{O}\mathrm{b}(\mathcal{C})$$

es una categoría con composición definida por $\overline{f} \circ \overline{g} = \overline{f \circ g}$.

La categoría $\widetilde{\mathcal{C}}$ se llama **categoría cociente** de $\mathcal{C}$ relativa a $\sim$, y se representa también por $\mathcal{C}/\sim$.

Ejemplos. 30.19.
(1) Sea $\mathcal{G}r$ la categoría de grupos. Para dos grupos A y B definimos en $\mathrm{Hom}_{\mathcal{G}r}(A,B)$ la relación $f_1 \sim f_2$ si existe $b \in B$ tal que $f_1(x) = bf_2(x)b^{-1}$ para $x \in A$. Obtenemos que la categoría cociente es la categoría de grupos y clases de conjugación de morfismos.
(2) La categoría de homotopía de espacios topológicos.

31. Funtores adjuntos

Una vez introducidos los conceptos básicos de la teoría de categorías, vamos a tratar los conceptos fundamentales de la misma: el de transformación natural y el de funtor adjunto.

Transformaciones naturales

Dados dos funtores $F, G : \mathcal{C} \to \mathcal{D}$ una **transformación natural** ó un **morfismo de funtores** de F a G es una aplicación $\nu : \mathcal{O}\mathrm{b}(\mathcal{C}) \to \cup \operatorname{Hom}_{\mathcal{D}}(D, D')$ verificando:

(I) Para cada objeto C de $\mathcal{C}$ se tiene que $\nu(C) \in \operatorname{Hom}_{\mathcal{D}}(F(C), G(C))$.
(II) Para cada morfismo $f : C \to C'$ de $\mathcal{C}$ se tiene $\nu(C')F(f) = G(f)\nu(C)$, esto es, el diagrama siguiente

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(C') \\ {\scriptstyle \nu(C)}\downarrow & & \downarrow{\scriptstyle \nu(C')} \\ G(C) & \xrightarrow{G(f)} & G(C') \end{array}$$

conmuta.

El funtor F se llama **dominio** de la transformación natural y G se llama el **codominio**. La transformación natural ν se representa entonces por $\nu : F \to G$, y gráficamente por

$$\mathcal{C} \underset{G}{\overset{F}{\rightrightarrows}} \mathcal{D} \quad \Downarrow \nu$$

Una transformación natural se llama un **isomorfismo natural** si para cada objeto C de $\mathcal{C}$ se tiene que $\nu(C)$ es un isomorfismo. Dos funtores se llaman **naturalmente isomorfos** si existe un isomorfismo natural de F a G.

Ejemplo. 31.1.

(1) Para cada funtor F existe una transformación natural id_F, definida, para cada objeto C de $\mathcal{C}$, por $\mathrm{id}_F(C) = \mathrm{id}_{F(C)}$.
(2) Existe una transformación natural del funtor identidad en $\mathcal{G}r$ al funtor abelianizado, con codominio en $\mathcal{G}r$. Para cada grupo G tenemos que $\nu(G)$ es la proyección canónica $G \to G_{ab}$.
(3) Si $\mathcal{C}$ es una categoría arbitraria y $f : B \to C$ un morfismo de $\mathcal{C}$, entonces existe una transformación natural $\nu : \operatorname{Hom}_{\mathcal{C}}(C, -) \longrightarrow \operatorname{Hom}_{\mathcal{C}}(B, -)$, definida por $\nu(A)(g) = g \circ f$ para cada $g \in \operatorname{Hom}_{\mathcal{C}}(C, A)$. También existe una transformación natural entre los funtores contravariantes $\mu : \operatorname{Hom}_{\mathcal{C}}(-, B) \longrightarrow \operatorname{Hom}_{\mathcal{C}}(-, C)$, definida por $\mu(A)(h) = f \circ h$ para cada $h \in \operatorname{Hom}_{\mathcal{C}}(A, B)$.

Se puede definir la composición de transformaciones naturales. Sean $\nu : F \to G$ y $\varepsilon : G \to H$ dos transformaciones naturales, definimos $\varepsilon \circ \nu : F \to H$ en la forma obvia, esto es, para cada objeto C de $\mathcal{C}$ tenemos: $(\varepsilon \circ \nu)(C) = \varepsilon(C) \circ \nu(C)$.

Lema. 31.2.
(1) La composición de transformaciones naturales es una transformación natural.
(2) La composición de transformaciones naturales es asociativa.
(3) Una transformación natural $\nu : F \to G$ es un **isomorfismo natural** *si, y sólo si, existe una transformación natural $\delta : G \to F$ tal que $\delta \circ \nu = id_F$ y $\nu \circ \delta = id_G$.*

Observación. 31.3.
Existe una quasicategoría que tiene por objetos los funtores y como morfismos las transformaciones naturales entre funtores.

Por comodidad si ν es una transformación natural y C es un objeto de $\mathcal{C}$, representamos $\nu(C)$ simplemente por ν_C. La composición $\nu_1 \circ \nu_2$ de dos transformaciones naturales ν_1 y ν_2 se representa simplemente por $\nu_1\nu_2$.

Composición estrella

Veamos a continuación otra forma de componer transformaciones naturales.

Proposición. 31.4.
Sean $F, G : \mathcal{C} \to \mathcal{D}$ y $H, K : \mathcal{D} \to \mathcal{E}$ funtores y sean $\nu : F \to G$ y $\gamma : H \to K$ transformaciones naturales.

$$\mathcal{C} \underset{G}{\overset{F}{\rightrightarrows}} \mathcal{D} \underset{K}{\overset{H}{\rightrightarrows}} \mathcal{E} \qquad (\Downarrow\nu,\ \Downarrow\gamma)$$

Entonces para cada objeto C de $\mathcal{C}$ el diagrama

$$\begin{array}{ccc} HF(C) & \xrightarrow{H(\nu_C)} & HG(C) \\ \gamma_{F(C)} \downarrow & & \downarrow \gamma_{G(C)} \\ KF(C) & \xrightarrow[K(\nu_C)]{} & KG(C) \end{array}$$

conmuta. Además, la diagonal

$$\mu_C = K(\nu_C)\gamma_{F(C)} = \gamma_{G(C)}H(\nu_C)$$

es una transformación natural $\mu : HF \to KG$.

Esta “composición" de transformaciones naturales se llama **composición estrella** y se representa por $\gamma \star \nu$.

Lema. 31.5.
(1) La composición estrella es asociativa.
(2) Para transformaciones naturales ν, γ, λ, μ verificando:

$$\mathcal{C} \underset{H}{\overset{F}{\underset{\Downarrow\gamma}{\overset{\Downarrow\nu}{\xrightarrow{G}}}}} \mathcal{D} \quad y \quad \mathcal{D} \underset{M}{\overset{K}{\underset{\Downarrow\mu}{\overset{\Downarrow\lambda}{\xrightarrow{L}}}}} \mathcal{E}$$

se tiene la igualdad:

$$(\mu\lambda) \star (\nu\gamma) = (\mu \star \gamma)(\lambda \star \nu).$$

Sea $F : \mathcal{C} \to \mathcal{D}$. Si usamos F para representar la transformación natural id_F, obtenemos:

Corolario. 31.6.
Para transformaciones naturales ν y γ verificando:

$$\mathcal{F} \underset{M}{\overset{L}{\Downarrow\gamma}} \mathcal{C} \xrightarrow{F} \mathcal{D} \underset{K}{\overset{H}{\Downarrow\nu}} \mathcal{E}$$

se verifica:
(1) $(\nu \star F)_C = \nu_{FC}$.
(2) $(F \star \gamma)_C = F(\gamma_C)$.

Corolario. 31.7. (Cinco reglas de Godement.)
Dada la siguiente situación de funtores y transformaciones naturales

$$\mathcal{C} \xrightarrow{L} \mathcal{D} \xrightarrow{K} \mathcal{E}\,, \quad \mathcal{E} \underset{W}{\overset{U}{\underset{\Downarrow\nu}{\overset{\Downarrow\xi}{\xrightarrow{V}}}}} \mathcal{F}\,, \quad \mathcal{F} \underset{H}{\overset{F}{\Downarrow\mu}} \mathcal{G} \xrightarrow{G} \mathcal{H}$$

los siguientes resultados son ciertos:
(1) $(GF) \star \xi = G \star (F \star \xi)$.
(2) $\xi \star (KL) = (\xi \star K) \star L$.

(3) $U \star K = UK$.
(4) $F \star (\xi \star K) = (F \star \xi) \star K$.
(5) $F \star (\nu\xi) \star K = (F \star \nu \star K)(F \star \xi \star K)$.
(6) El siguiente cuadrado es conmutativo:

$$\begin{array}{ccc} FU & \xrightarrow{F\star\xi} & FV \\ {\scriptstyle \mu\star U}\downarrow & & \downarrow{\scriptstyle \mu\star V} \\ HU & \xrightarrow{H\star\xi} & HV \end{array}$$

Observación. 31.8.
Existe una quasicategoría cuyos objetos son las categorías y los morfismos son las transformaciones naturales.

$$\mathcal{C} \underset{G}{\overset{F}{\rightrightarrows}} \mathcal{D} \quad (\Downarrow \nu)$$

El dominio de ν es $\mathcal{C}$ y el codominio es $\mathcal{D}$. La composición es la composición estrella.
Ejemplos. 31.9.
(1) Los siguientes funtores F y G son naturalmente isomorfos.

$$F, G : \mathcal{S}et^{op} \times \mathcal{S}et^{op} \times \mathcal{S}et \to \mathcal{S}et; \quad \begin{cases} F(A,B,C) = \operatorname{Hom}(A \times B, C), \\ G(A,B,C) = \operatorname{Hom}(A, \operatorname{Hom}(B,C)). \end{cases}$$

(2) Los siguientes funtores son naturalmente isomorfos.

$$\begin{array}{l} \operatorname{Hom}(\{0,1\}, -) : \mathcal{S}et \to \mathcal{S}et, \\ (-)^2 : \mathcal{S}et \to \mathcal{S}et. \end{array}$$

(3) Un endomorfismo de grupos es un automorfismo interior si, y sólo si, considerado como funtor sobre la categoría de un único objeto es naturalmente isomorfo al funtor identidad.
(4) Los funtores grupo libre y grupo abeliano libre no son naturalmente isomorfos, pero existe entre ellos una transformación natural.

Isomorfismo de categorías

Un funtor $F : \mathcal{C} \to \mathcal{D}$ es un **isomorfismo** de $\mathcal{C}$ a $\mathcal{D}$ si es un isomorfismo en la quasicategoría de todas las categorías. Esto es, si existe un funtor $G : \mathcal{D} \to \mathcal{C}$ tal que $F \circ G = \mathrm{id}_{\mathcal{D}}$ y $G \circ F = \mathrm{id}_{\mathcal{C}}$. Dos categorías $\mathcal{C}$ y $\mathcal{D}$ se llaman **isomorfas** si existe un isomorfismo $F : \mathcal{C} \to \mathcal{D}$.

Ejemplos. 31.10.
(1) Todo funtor identidad es un isomorfismo.
(2) El funtor $\mathcal{R}\mathrm{ing} \to \mathcal{R}\mathrm{ing}$ definido por $R \mapsto R^{op}$ es un isomorfismo.

(3) La categoría de anillos es isomorfa a la de $\mathbb{Z}$–álgebras.
(4) La categoría $\mathcal{M}on$ de monoides **no** es isomorfa a una subcategoría de la categoría de semigrupos $\mathcal{S}gr$.

Un funtor $F : \mathcal{C} \to \mathcal{D}$ es **pleno** si para cada $C_1, C_2 \in \mathcal{O}\mathrm{b}(\mathcal{C})$ se tiene la igualdad $F(\mathrm{Hom}_{\mathcal{C}}(C_1, C_2)) = \mathrm{Hom}_{\mathcal{D}}(F(C_1), F(C_2))$, y es **fiel** si $F : \mathrm{Hom}_{\mathcal{C}}(C_1, C_2) \to \mathrm{Hom}_{\mathcal{D}}(F(C_1), F(C_2))$ es una aplicación inyectiva para cualesquiera $C_1, C_2 \in \mathcal{O}\mathrm{b}(\mathcal{C})$.

Proposición. 31.11.
Sea $F : \mathcal{C} \to \mathcal{D}$ es un funtor. Son equivalentes los siguientes enunciados:
(a) F es un isomorfismo.
(b) F es una biyección entre morfismos.
(c) F es pleno y fiel y la función objeto es una biyección.

Desde un punto de vista teórico el concepto de isomorfismo funtorial es de interés, pero más importante es el de equivalencia de categoría, pues nos interesa más relacionar categorías que tengan propiedades comunes, aunque no sean isomorfas. Por ejemplo la categoría de espacios vectoriales de dimensión finita sobre un cuerpo K no es isomorfa a la categoría introducida en el Ejemplo (30.5.), cuando tomamos $R = K$, pero ambas categorías son muy parecidas. Este parecido lo refleja con claridad el concepto de equivalencia de categorías.

Equivalencia de categorías

Una categoría $\mathcal{C}$ se llama **esquelética** si dos objetos que son isomorfos son iguales. Se llama **esqueleto** de una categoría $\mathcal{C}$ a una subcategoría plena esquelética y maximal de $\mathcal{C}$.

Proposición. 31.12.
Toda categoría tiene un esqueleto.

Proposición. 31.13.
Cada dos esqueletos de una categoría son isomorfos.

Dos categorías $\mathcal{C}$ y $\mathcal{D}$ se llaman **equivalentes** si tienen esqueletos isomorfos. La relación "ser equivalente" es una relación de equivalencia en la quasicategoría de todas las categorías.

Proposición. 31.14.
Dos categorías esqueléticas son equivalentes si, y sólo si, son isomorfas.

Teorema. 31.15.
Sea $F : \mathcal{C} \to \mathcal{D}$ un funtor. Son equivalentes los siguientes enunciados:
(a) F es pleno, fiel y denso.
(b) Existe un funtor $G : \mathcal{D} \to \mathcal{C}$ tal que $FG \cong \mathrm{id}_{\mathcal{D}}$ y $GF \cong \mathrm{id}_{\mathcal{C}}$.
(c) Existe un funtor $G : \mathcal{D} \to \mathcal{C}$ e isomorfismos naturales $\nu : \mathrm{id}_{\mathcal{C}} \to GF$, $\epsilon : FG \to \mathrm{id}_{\mathcal{D}}$ tales que $F \star \nu = (\epsilon \star F)^{-1}$ y $G \star \epsilon = (\nu \star G)^{-1}$.

Un funtor $F : \mathcal{C} \to \mathcal{D}$ se llama una **equivalencia** si verifica las condiciones equivalentes del Teorema anterior.

Lema. 31.16.
(1) La composición de equivalencias es una equivalencia.
(2) Si F es una equivalencia, entonces también F^{op} lo es.
(3) Si F es una equivalencia, con funtor en sentido contrario G, entonces G es una equivalencia.

Lema. 31.17.
Si $\mathcal{S}$ es un esqueleto de una categoría $\mathcal{C}$ y $E : \mathcal{S} \to \mathcal{C}$ es el funtor inclusión, entonces existe un funtor $P : \mathcal{C} \to \mathcal{S}$ tal que $PE = \mathrm{id}_{\mathcal{S}}$ y tanto P como E son equivalencias.

Teorema. 31.18.
Si $\mathcal{C}$ y $\mathcal{D}$ son categorías, son equivalentes los siguientes enunciados:
(a) $\mathcal{C}$ y $\mathcal{D}$ son equivalentes.
(b) Existe una equivalencia $F : \mathcal{C} \to \mathcal{D}$.

Ejemplos. 31.19.
(1) Todo isomorfismo de categorías es una equivalencia.

(2) Todo funtor naturalmente isomorfo a un isomorfismo de categorías es una equivalencia. (El recíproco no es cierto.)
(3) Si K es un cuerpo y $\mathcal{C}$ es la categoría de los K–espacios vectoriales finito–dimensionales, entonces $\mathrm{Hom}_{\mathcal{C}}(-,K) : \mathcal{C}^{op} \to \mathcal{C}$ es una equivalencia y no es un isomorfismo.

Observación. 31.20.
El concepto de equivalencia es más importante que el de isomorfismo, ya que las equivalencias preservan y reflejan todas las propiedades categóricas esenciales. Es más, incluso podrían definirse las propiedades categóricas como aquellas que son preservadas por equivalencias.

Dos categorías $\mathcal{C}$ y $\mathcal{D}$ se llaman **dualmente equivalentes** si $\mathcal{C}^{op}$ y $\mathcal{D}$ son equivalentes.
Una categoría $\mathcal{C}$ se llama **autodual** si es dualmente equivalente a sí misma.

Funtores adjuntos

Sean $\mathcal{C}$ y $\mathcal{D}$ dos categorías y

$$\begin{array}{c} \mathcal{C} \\ F \Big\downarrow \Big\uparrow G \\ \mathcal{D} \end{array}$$

dos funtores. Decimos que F es un **adjunto a la izquierda** del funtor G, ó que G es un **adjunto a la derecha** del funtor F si existe un isomorfismo natural

$$\eta_{X,Y} : \mathrm{Hom}_{\mathcal{D}}(FX,Y) \cong \mathrm{Hom}_{\mathcal{C}}(X,GY).$$

η se llama el **isomorfismo de la adjunción** y es una transformación natural de funtores. La situación anterior se representa abreviadamente por:

$$\eta : F \dashv G.$$

Ejemplo. 31.21.
Consideramos el funtor de olvido $U : R\text{–}\boldsymbol{Mod} \to \mathcal{S}et$, entonces el funtor R–módulo libre es un adjunto a la izquierda de U.

$$\begin{array}{c} \mathcal{S}et \\ R^{(-)} \Big\downarrow \Big\uparrow U \\ R\text{–}\boldsymbol{Mod} \end{array}$$

Proposición. 31.22.
Sean

$$\begin{array}{c} \mathcal{C} \\ F_1 \Big\downarrow \Big\uparrow G_1 \\ \mathcal{D} \end{array} \quad y \quad \begin{array}{c} \mathcal{D} \\ F_2 \Big\downarrow \Big\uparrow G_2 \\ \mathcal{E} \end{array}$$

categorías y funtores. Si $\eta_1 : F_1 \dashv G_1$ *y* $\eta_2 : F_2 \dashv G_2$*, entonces*

$$\eta_1\eta_2 : F_2F_1 \dashv G_1G_2$$

es una adjunción.

Consideramos la adjunción $\eta : F \dashv G$, esto es,

$$\begin{array}{c}\mathcal{C}\\ F\Big\downarrow\Big\uparrow G\\ \mathcal{D}\end{array}$$

La naturalidad de η significa la conmutatividad del siguiente diagrama:

$$\begin{array}{ccc}\mathrm{Hom}_{\mathcal{D}}(FX,Y) & \xrightarrow{\eta_{X,Y}} & \mathrm{Hom}_{\mathcal{C}}(X,GY)\\ {\scriptstyle (Ff)^{\star}g_{\star}}\Big\downarrow & & \Big\downarrow{\scriptstyle f^{\star}(Gg)_{\star}}\\ \mathrm{Hom}_{\mathcal{D}}(FZ,T) & \xrightarrow{\eta_{Z,T}} & \mathrm{Hom}_{\mathcal{C}}(Z,GT)\end{array}$$

para $f : Z \to X$ y $g : Y \to T$. Entonces para cada $\alpha \in \mathrm{Hom}_{\mathcal{D}}(FX,Y)$ se verifica la igualdad de las siguientes expresiones:

$$f^{\star}(Gg)_{\star}\eta_{X,Y}(\alpha) = (Gg)\eta(\alpha)f$$

$$\eta_{Z,T}(Ff)^{\star}g_{\star}(\alpha) = \eta(g\alpha(Ff))$$

Y en consecuencia tenemos:

$$\eta(g\alpha(Ff)) = (Gg)\eta(\alpha)f$$

Existen dos casos especiales:

(1) Tomando $Y = FX$ y $\alpha = \mathrm{id}_{FX}$, entonces

$$\eta(\mathrm{id}_{FX}) = \varepsilon_X : X \to GFX$$

se llama la **unidad** de la adjunción.

(2) Tomando $X = GY$ y $\mathrm{id}_{GY} \in \mathrm{Hom}_{\mathcal{C}}(GY,GY)$, entonces

$$\eta^{-1}(\mathrm{id}_{GY}) = \delta_Y : FGY \to Y$$

se llama la **counidad** de la adjunción.

Tanto ε como δ son transformaciones naturales. Vamos a ver qué relaciones verifican ε y δ.
Tenemos:

$$\eta(\delta_{FX}F\varepsilon_X) = \eta(\delta_{FX})\varepsilon_X = \eta\eta^{-1}(\mathrm{id}_{GFX})\varepsilon_X = \varepsilon_X = \eta(\mathrm{id}_{FX}).$$

Luego tenemos:

$$\delta F \circ F\varepsilon = F.$$

$$\begin{array}{ccc} F & \xrightarrow{F\varepsilon} & FGF \\ & \searrow^{F} & \downarrow \delta F \\ & & F \end{array}$$

De la misma forma tenemos:

$$\eta^{-1}(G\delta_Y \circ \varepsilon G_Y) = \eta^{-1}\eta(\delta_Y \,\mathrm{id}_{FGY}) = \delta_Y = \eta^{-1}(\mathrm{id}_{GY}).$$

Luego tenemos:

$$G\delta \circ \varepsilon G = G.$$

$$\begin{array}{ccc} G & \xrightarrow{\varepsilon G} & GFG \\ & \searrow^{G} & \downarrow G\delta \\ & & G \end{array}$$

Las descripciones así obtenidas nos permiten además dar descripciones alternativas de η y η^{-1}.

$$\eta(\alpha) = \eta(\alpha \,\mathrm{id}_{FX}) = G(\alpha)\eta(\mathrm{id}_{FX}) = G(\alpha)\varepsilon_X.$$

$$\eta^{-1}(\beta) = \eta^{-1}(\mathrm{id}_{GY}\,\beta) = \eta^{-1}(\eta(\delta_Y)\beta) = \delta_Y F(\beta).$$

Proposición. 31.23.
Sean

$$\mathcal{C} \underset{G}{\overset{F}{\rightleftarrows}} \mathcal{D}$$

categorías y funtores. Supongamos que

$$\varepsilon : id_{\mathcal{C}} \to GF \qquad y \qquad \delta : FG \to id_{\mathcal{D}}$$

son transformaciones naturales verificando las relaciones:

$$\delta F \circ F\varepsilon = id_{\mathcal{C}} \qquad y \qquad G\delta \circ \varepsilon G = id_{\mathcal{D}},$$

entonces

$$\eta : \mathrm{Hom}_{\mathcal{D}}(FX, Y) \to \mathrm{Hom}_{\mathcal{C}}(X, GY)$$

definido por $\eta(\alpha) = G(\alpha)\varepsilon_X$ *para cada* $\alpha \in \mathrm{Hom}_{\mathcal{D}}(FX, Y)$, *define una adjunción* $F \dashv G$ *de forma que la unidad es* ε *y la counidad es* δ.

El siguiente paso es demostrar que en una adjunción $F \dashv G$ el funtor G está determinado salvo equivalencia natural.

Proposición. 31.24.
Sea $\eta : F \dashv G$ una situación de adjunción, si $\eta' : F \dashv G'$ es otra situación de adjunción, existe una equivalencia natural $\theta : G \to G'$.

La proposición anterior se completa como sigue:

Proposición. 31.25.
Sean $\eta : F \dashv G$ y $\eta' : F \dashv G'$ situaciones de adjunción y sea $\theta : G \to G'$ la equivalencia natural construida en la Proposición anterior. Entonces se verifica:
(1) $\theta F \circ \varepsilon = \varepsilon'$.
(2) $\delta \circ F\overline{\theta} = \delta'$.
(3) $\theta_Y \circ \eta(f) = \eta'(f)$ para cada $f \in \operatorname{Hom}_{\mathcal{D}}(FX, Y)$.

Y recíprocamente, si $\eta : T \dashv G$ es una situación de adjunción y $\theta : G \to G'$ es una equivalencia natural, entonces $\eta' : F \dashv G'$, definida $\eta'(f) = \theta_Y \circ \eta(f)$ es una adjunción, la unidad de la adjunción es $\varepsilon = \theta F \circ \varepsilon$ y la counidad es $\delta' = \delta \circ F\theta$.

Proposición. 31.26.
Si $F : \mathcal{C} \to \mathcal{D}$ es un funtor pleno y fiel, y si $F \dashv G$ es una situación de adjunción, entonces $\varepsilon : id_{\mathcal{C}} \to GF$ es una equivalencia natural.

Proposición. 31.27.
Si $F : \mathcal{C} \to \mathcal{D}$ es un embebimiento pleno y si $F \dashv G$ es una situación de adjunción, entonces existe un funtor G' y una adjunción $F \dashv G'$ tal que la unidad $\varepsilon' : id_{\mathcal{C}} \to G'F$ es la identidad.

32. Funtores Hom y producto tensor

Funtor Hom covariante

Dado un anillo (conmutativo) A, para cada A–módulo M existe un funtor

$$\mathrm{Hom}_A(M,-) : A\text{–}\boldsymbol{Mod} \longrightarrow A\text{–}\boldsymbol{Mod},$$

para cada homomorfismo $f : X \longrightarrow Y$ tenemos un homomorfismo

$$\mathrm{Hom}_A(M,f) : \mathrm{Hom}_A(M,X) \longrightarrow \mathrm{Hom}_A(M,Y),$$

definido $\mathrm{Hom}_A(M,f)(h) = f \circ h$, para cada $h \in \mathrm{Hom}_A(M,X)$. En ciertas ocasiones conviene representar a $\mathrm{Hom}_A(M,f)$ simplemente por f_*; en este caso se tiene $f_*(h) = f \circ h$

Lema. 32.1.
Dado un anillo conmutativo A y dos A–módulos M y N, el conjunto $\mathrm{Hom}_A(M,N)$, de los homomorfismos de A–módulos de M a N, tiene estructura de A–módulo, con acción dada por

$$(af)(m) = af(m),$$

para cualesquiera $a \in A, f \in \mathrm{Hom}_A(M,N)$ y $m \in M$.

Una transformación natural

Dado un homomorfismo de A–módulos $g : N \longrightarrow M$, para cada A–módulo X tenemos un homomorfismo

$$\mathrm{Hom}_A(M,X) \stackrel{(g^*)_X}{\longrightarrow} \mathrm{Hom}_A(N,X),$$

definido $(g^*)_X(h) = h \circ g$ para cada $h \in \mathrm{Hom}_A(M,X)$. De esta forma g^* define una transformación natural de $\mathrm{Hom}_A(M,-)$ a $\mathrm{Hom}_A(N,-)$ que asigna a cada A–módulo X el homomorfismo $(g^*)_X : \mathrm{Hom}_A(M,X) \longrightarrow \mathrm{Hom}_A(N,X)$, de forma que para cada homomorfismo $f : X \longrightarrow Y$ se tiene un diagrama conmutativo

$$\begin{array}{ccc}
\mathrm{Hom}_A(M,X) & \xrightarrow{(g^*)_X} & \mathrm{Hom}_A(N,X) \\
{\scriptstyle (f_*)_M}\downarrow & & \downarrow{\scriptstyle (f_*)_N} \\
\mathrm{Hom}_A(M,Y) & \xrightarrow{(g^*)_Y} & \mathrm{Hom}_A(N,Y)
\end{array}$$

Funtor Hom contravariante

Esto sugiere que podemos definir un nuevo funtor $\mathrm{Hom}_A(-,X) : A-\boldsymbol{Mod} \longrightarrow A-\boldsymbol{Mod}$ en la forma obvia. Pero observar que si $M \xrightarrow{g} N \xrightarrow{g'} P$ son homomorfismos de A–módulos, entonces tenemos para cada A–módulo X

$$\mathrm{Hom}_A(P,X) \xrightarrow{(g'^*)_X} \mathrm{Hom}_A(N,X) \xrightarrow{(g^*)_X} \mathrm{Hom}_A(M,X),$$

y observar que $(g^*)_X \circ (g'^*)_X = ((g' \circ g)^*)_X$ esto es, $\mathrm{Hom}_A(-,X)$ es un funtor contravariante.

Bifuntor Hom covariante

Finalmente podemos considerar

$$\mathrm{Hom}_A(-,-) : A-\boldsymbol{Mod}^{op} \times A-\boldsymbol{Mod} \longrightarrow A-\boldsymbol{Mod}.$$

De esta forma se obtiene un bifuntor, y observar que se tiene:

Proposición. 32.2.
Sea A un anillo, existe un bifuntor

$$\mathrm{Hom}_A(-,-) : A-\boldsymbol{Mod} \times A-\boldsymbol{Mod} \longrightarrow A-\boldsymbol{Mod},$$

que es covariante en la segunda variable y contravariante en la primera. Esto es, tenemos un diagrama conmutativo para cualesquiera $f : M_1 \to M_2$ y $g : N_1 \to N_2$.

$$\begin{array}{ccc} \mathrm{Hom}_A(N_2,M_1) & \xrightarrow{f_*} & \mathrm{Hom}_A(N_2,M_2) \\ \downarrow g^* & & \downarrow g^* \\ \mathrm{Hom}_A(N_1,M_1) & \xrightarrow{f_*} & \mathrm{Hom}_A(N_1,M_2) \end{array}$$

Producto tensor

Dados A–módulos M_1, M_2 y N estamos interesados en las aplicaciones de $M_1 \times M_2 \longrightarrow N$ que son lineales en las dos variables y que verifican la propiedad adicional (iii).

$$f : M_1 \times M_2 \longrightarrow N,$$

(I) $f(m_1 + m_1', m_2) = f(m_1, m_2) + f(m_1', m_2)$,
(II) $f(m_1, m_2 + m_2') = f(m_1, m_2) + f(m_1, m_2')$,

(III) $f(m_1a,m_2) = af(m_1,m_2) = f(m_1,am_2)$

Para cualesquiera $m_1,m_1' \in M_1$, cualesquiera $m_2,m_2' \in M_2$ y cualquiera $a \in A$. Una aplicación f verificando (i), (ii) y (iii) se llama A**–bilineal**.

Para determinar todas estas aplicaciones vamos a construir un nuevo A–módulo. Para ello definimos un A–módulo libre F sobre el conjunto $M_1 \times M_2$ y hacemos el cociente por el submódulo generado por los elementos:

$$\{(m_1+m_1',m_2)-(m_1,m_2)-(m_1',m_2),(m_1,m_2+m_2')-(m_1,m_2)-(m_1,m_2'),\\ (m_1a,m_2)-a(m_1,m_2),(m_1,am_2)-a(m_1,m_2) \mid\ m_1,m_1' \in M_1,m_2,m_2' \in M_2,a \in A\}$$

Si llamamos $M_1 \otimes_A M_2$ este módulo cociente, y la clase de (m_1,m_2) la representamos por $m_1 \otimes m_2$, entonces existe una aplicación A–bilineal

$$t : M_1 \times M_2 \longrightarrow M_1 \otimes M_2, \quad t(m_1,m_2) = m_1 \otimes m_2.$$

Además el par $(t,M_1 \otimes_A M_2)$ verifica la siguiente propiedad.

Proposición. 32.3. (Propiedad universal del producto tensor.)
Para cualesquiera A–módulos M_1,M_2 y N y cualquier aplicación lineal $f : M_1 \times M_2 \longrightarrow N$ existe un homomorfismo de A–módulos $f' : M_1 \otimes_A M_2 \longrightarrow N$ tal que $f = f' \circ t$. Esto es, el siguiente diagrama conmuta

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{t} & M_1 \otimes_A M_2 \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f'} & \\ & N & \end{array}$$

Los elementos de $M_1 \otimes_A M_2$ son combinaciones lineales del tipo $\sum_{i=1}^n m_{1i} \otimes m_{2i}$.

Proposición. 32.4.
Para cualesquiera A–módulos M_1,M_2,M_3 y M se verifica:

(1) $M_1 \otimes_A M_2 \cong M_2 \otimes_A M_1$.
(2) $A \otimes_A M \cong M$.
(3) $M_1 \otimes_A (M_2 \otimes_A M_3) \cong (M_1 \otimes_A M_2) \otimes_A M_3$.

Proposición. 32.5.
Si $f_1 : M_1 \longrightarrow N_1$ y $f_2 : M_2 \longrightarrow N_2$ son homomorfismos de A–módulos, entonces existe un único homomorfismo de A–módulos $f_1 \otimes_A f_2 : M_1 \otimes_A M_2 \longrightarrow N_1 \otimes_A N_2$ tal que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{t} & M_1 \otimes_A M_2 \\ {\scriptstyle f_1 \times f_2}\downarrow & & \downarrow {\scriptstyle f_1 \otimes_A f_2} \\ N_1 \times N_2 & \xrightarrow{t} & N_1 \otimes_A N_2. \end{array}$$

La definición de $f_1 \otimes_A f_2$ sobre los generadores de $M_1 \otimes_A M_2$ es: $(f_1 \otimes_A f_2)(m_1 \otimes m_2) = f_1(m_1) \otimes f_2(m_2)$.

Una nota sobre notación. Para cada homomorfismo $f_2 : M_2 \longrightarrow N_2$ y cada A–módulo M_1 representamos $\mathrm{id}_{M_1} \otimes_A f_2$ simplemente por $M_1 \otimes f_2$.

Teorema. 32.6.
Existe un bifuntor $- \otimes_A - : A-\boldsymbol{Mod} \times A-\boldsymbol{Mod} \longrightarrow A-\boldsymbol{Mod}$.

Lema. 32.7.
Sean $f_i : M_i \to N_i$, $i = 1, 2$, homomorfismos sobreyectivos, entonces:
(1) $f_1 \otimes f_2$ es un homomorfismo sobreyectivo.
(2) $\mathrm{Ker}(f_1 \otimes f_2) = \{\sum x_j \otimes y_j \mid x_j \in \mathrm{Ker}(f_1)$ ó $y_j \in \mathrm{Ker}(f_2)\}$.

DEMOSTRACIÓN. (2). Llamamos $H = \{\sum x_j \otimes y_j \mid x_j \in \mathrm{Ker}(f_1)$ ó $y_j \in \mathrm{Ker}(f_2)\}$, es claro que $H \subseteq \mathrm{Ker}(f_1 \otimes f_2)$. Tenemos entonces un homomorfismo $h : M_1 \otimes_A M_2/H \longrightarrow N_1 \otimes_A N_2$ definido $h(x \otimes y) = f_1(x) \otimes f_2(y)$, y $\mathrm{Ker}(h) = \mathrm{Ker}(f_1 \otimes f_2)/H$.

Definimos $f : N_1 \times N_2 \to M_1 \otimes_A M_2/H$ mediante $f(u, v) = x \otimes y + H$, siendo $f_1(x) = u$ y $f_2(y) = v$; vamos a ver que f está bien definida. Si $x' \in M_1$ e $y' \in M_2$ verifican $f_1(x') = u$ y $f_2(y') = v$, entonces

$$x \otimes y - x' \otimes y' = x \otimes (y - y') + (x - x') \otimes y \in H.$$

Tenemos que f es bilineal, y por tanto existe un único homomorfismo $f' : N_1 \otimes_A N_2 \to M_1 \otimes_A M_2/H$ que es inverso de h. Luego $M_1 \otimes_A M_2/H = M_1 \otimes_A M_2/\mathrm{Ker}(f_1 \otimes f_2)$, y por tanto $H = \mathrm{Ker}(f_1 \otimes f_2)$. □

Proposición. 32.8.
Para cada módulo M, y cada submódulo $N_1 \subseteq N$ se tiene que la sucesión

$$M \otimes_A N_1 \to M \otimes_A N \to M \otimes_A N/N_1 \to 0$$

es exacta.

DEMOSTRACIÓN. Consideramos las aplicaciones $N_1 \xrightarrow{f} N \xrightarrow{g} N/N_1 \to 0$. Seguimos los siguientes pasos:

(1) $M \otimes g$ es sobreyectiva. Para cada $m \otimes n + N_1$ tenemos que $m \otimes n + N_1 = M \otimes g(m \otimes n)$.
(2) $(M \otimes g) \circ (M \otimes f) = M \otimes (g \circ f) = 0$.
(3) $\mathrm{Ker} := \mathrm{Ker}(M \otimes g) \subseteq \mathrm{Im}(M \otimes f) =: \mathrm{Im}$. Como $\mathrm{Im} \subseteq \mathrm{Ker}$, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} M \otimes N & \longrightarrow & M \otimes (N/N_1) \\ & \searrow \quad \nearrow_{t} & \\ & \frac{M\otimes N}{\mathrm{Im}} & \\ \nearrow & & \\ \frac{\mathrm{Ker}}{\mathrm{Im}} & & \end{array}$$

siendo $\frac{\mathrm{ker}}{\mathrm{Im}} = \mathrm{Ker}(t)$, definida $t(m \otimes n + \mathrm{Im}) = m \otimes (n + N_1)$. Por ser g sobreyectiva, se tiene que t es sobreyectiva.

Definimos $\phi : M \times (N/N_1) \to \frac{M\otimes N}{\mathrm{Im}}$ mediante $\phi(m, n+N_1) = (m\otimes n)+\mathrm{Im}$; es claro que es A–bilineal y que define un homomorfismo $k : M \otimes (N/N_1) \to \frac{M\otimes N}{\mathrm{Im}}$ mediante $k(m \otimes (n+N_1)) = (m \otimes n) + \mathrm{Im}$.

Vamos a ver que k es inversa de t. Para ello basta comprobar que $k \circ t = \mathrm{id}$. Tenemos $(k \circ t)((m \otimes n) + \mathrm{Im}) = k(m \otimes (n + N_1)) = (m \otimes n) + \mathrm{Im}$. En consecuencia $\mathrm{Ker}(t) = 0$ y se tiene $\mathrm{Ker} = \mathrm{Im}$.

□

Extensión y restricción de escalares

Si $h : A \longrightarrow B$ es un homomorfismo de anillos, cada B–módulo M es un A–módulo via la restricción de escalares, esto es, la estructura de A–módulo de M está dada por:

$$am = h(a)m$$

para cada $a \in A$ y cada $m \in M$.

Lema. 32.9.
Para cada homomorfismo de anillos $h : A \longrightarrow B$ *existe un funtor* $\mathcal{U}_h : B\text{–}\textbf{\textit{Mod}} \longrightarrow A\text{–}\textbf{\textit{Mod}}$, *el* ***funtor restricción de escalares***.

Podemos construir B–módulos a partir de A–módulos utilizando el producto tensor. Si N es un A–módulo y M un B–módulo, en $M \otimes_A N$ podemos dar una estructura de B–módulo mediante:

$$b(m \otimes n) = (bm) \otimes n.$$

para cada $b \in B$, $m \in M$ y $n \in N$. En particular, para cada A–módulo N tenemos que $B \otimes_A N$ es un B–módulo.

Lema. 32.10.
Para cada homomorfismo de anillos $h_A \longrightarrow B$ *existe un funtor* $B \otimes_A - : A\text{–}\textbf{\textit{Mod}} \longrightarrow B\text{–}\textbf{\textit{Mod}}$, *el* ***funtor extensión de escalares***.

Teorema. 32.11.
Existe una adjunción

$$\begin{array}{c} A\text{–}\textbf{\textit{Mod}} \\ {\scriptstyle B\otimes_A -}\downarrow\ \uparrow{\scriptstyle \mathcal{U}_h} \\ B\text{–}\textbf{\textit{Mod}} \end{array},$$

donde $\mathcal{U}_h : B\text{–}\textbf{\textit{Mod}} \longrightarrow A\text{–}\textbf{\textit{Mod}}$ *es el funtor cambio de anillo.*

Existe una situación de adjunción similar para el funtor Hom.

Proposición. 32.12.
Para cada homomorfismo de anillos $h : A \longrightarrow B$.
(1) Existe un funtor $\operatorname{Hom}_A(B, -) : A\text{–}\textbf{\textit{Mod}} \longrightarrow B\text{–}\textbf{\textit{Mod}}$.
(2) Existe una situación de adjunción

$$\begin{array}{c} B\text{–}\textbf{\textit{Mod}} \\ {\scriptstyle \mathcal{U}_h}\downarrow\ \uparrow{\scriptstyle \operatorname{Hom}_A(B,-)} \\ A\text{–}\textbf{\textit{Mod}} \end{array}$$

Citamos finalmente una situación de adjunción especialmente de interés.

Proposición. 32.13.
Para cada A–módulo M existe una situación de adjunción

$$\begin{array}{c} A\text{–}\boldsymbol{Mod} \\ M\otimes_A - \Big\downarrow \Big\uparrow \operatorname{Hom}_A(M,-) \\ A\text{–}\boldsymbol{Mod} \end{array}$$

DEMOSTRACIÓN. Consideramos el diagrama

$$\operatorname{Hom}_A(M\otimes_A X, Y) \stackrel{b}{\longrightarrow} \operatorname{Hom}_A(X, Hom_A(M,Y)),$$

donde b está definido $b(f)(x)(m) = f(m\otimes x)$, con inversa b^{-1}, definida $b^{-1}(g)(m\otimes x) = g(x)(m)$. □

Álgebras

Dado un anillo A y dos A–álgebras (conmutativas) R y S, se considera el producto tensor $R\otimes_A S$. En principio tenemos un A–módulo, pero de forma natural existe una estructura de A–álgebra en $R\otimes_A S$ con producto

$$(r_1\otimes s_1)(r_2\otimes s_2) = (r_1r_2)\otimes(s_1s_2).$$

Con esta estructura existen homomorfismos de A–álgebras

$$\begin{array}{ll} j_R : R \longrightarrow R\otimes_A S, & j_R(r) = r\otimes 1, \\ j_S : S \longrightarrow R\otimes_A S, & j_S(s) = 1\otimes s. \end{array}$$

Lema. 32.14.
Dadas dos A–álgebras (conmutativas) R y S, el par $(R\otimes_A S, \{j_r, j_s\})$ es una suma directa de R y S en la categoría de A–álgebras.

Ejercicio. 32.15.
Dado un anillo A e indeterminadas X e Y, existe un isomorfismo de A–álgebras $A[X]\otimes_A A[Y] \cong A[X,Y]$.

33. Sucesiones exactas

En esta sección vamos a tratar con A–módulos y homomorfismos de A–módulos.
Una **sucesión** de homomorfismos es una lista de homomorfismos indizada en $\mathbb{Z}$, por ejemplo $\{f_i \mid i \in \mathbb{Z}\}$ tal que es posible hacer las composiciones $f_{i+1} \circ f_i$ para cada $i \in \mathbb{Z}$.

$$\dots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \cdots \qquad \text{(V.1)}$$

La sucesión (V.1) es **exacta** en M_i si $\operatorname{Im}(f_{i-1}) = \operatorname{Ker}(f_i)$. Y la sucesión (V.1) es **exacta** si es exacta en cada M_i.
La sucesión (V.1) es **acotada a izquierda** si existe un índice k tal que $M_i = 0$ para cada $i \leq k$, y es **acotada a derecha** si existe un índice h tal que $M_i = 0$ para cada $i \geq h$. Si la sucesión (V.1) es acotada a izquierda para $k = -1$ escribimos simplemente:

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} \cdots \qquad \text{(V.2)}$$

La sucesión (V.1) es **exacta corta** si es exacta y $M_i = 0$ para cada $i < 0$ y $i \geq 3$. Por lo tanto f_1 es inyectiva, f_2 es sobreyectiva e $\operatorname{Im}(f_1) = \operatorname{Ker}(f_2)$. Escribimos

$$0 \longrightarrow M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \longrightarrow 0 \qquad \text{(V.3)}$$

Ejemplo. 33.1.
Si $N \subseteq M$ es un submódulo, entonces

$$0 \to N \stackrel{incl.}{\to} M \to M/N \to 0$$

es una sucesión exacta corta.

Ejemplo. 33.2.
Si M_1 y M_2 son A–módulos, entonces $0 \to M_1 \stackrel{j_1}{\to} M_1 \oplus M_2 \stackrel{p_2}{\to} M_2 \to 0$ es una sucesión exacta corta.

Ejemplo. 33.3.
Si $f : M \to M'$ es un homomorfismo de A–módulos, entonces

$$0 \to \operatorname{Ker}(f) \stackrel{incl.}{\to} M \stackrel{f}{\to} M' \stackrel{proy.}{\to} \frac{M'}{\operatorname{Im}(f)} \to 0$$

es una sucesión exacta.

Dadas dos sucesiones $\mathbb{M} := \{M_i, f_i \mid i \in \mathbb{Z}\}$ y $\mathbb{N} := \{N_i, g_i \mid i \in \mathbb{Z}\}$ un **homomorfismo** de $\mathbb{M}$ a $\mathbb{N}$ es una familia de homomorfismos de A–módulos $h := \{h_i \mid i \in \mathbb{Z}\}$ tal que el diagrama

$$\begin{array}{ccccccccc}
\dots & \xrightarrow{f_{i-1}} & M_{i-1} & \xrightarrow{f_i} & M_i & \xrightarrow{f_{i+1}} & M_{i+1} & \xrightarrow{f_{i+2}} & \dots \\
 & & \downarrow{h_{i-1}} & & \downarrow{h_i} & & \downarrow{h_{i+1}} & & \\
\dots & \xrightarrow{g_{i-1}} & N_{i-1} & \xrightarrow{g_i} & N_i & \xrightarrow{g_{i+1}} & N_{i+1} & \xrightarrow{g_{i+2}} & \dots
\end{array}$$

es conmutativo, esto es, para cada índice $i \in \mathbb{Z}$ se tiene: $h_i \circ f_i = g_i \circ h_{i-1}$.

Las sucesiones $\mathbb{M}$ y $\mathbb{N}$ son **equivalentes** si existe un homomorfismo $h : \mathbb{M} \to \mathbb{N}$ tal que cada h_i es un isomorfismo.

Lema. 33.4.
Cada sucesión exacta corta es equivalente a una sucesión exacta corta definida por un submódulo, ver Ejemplo (33.1.).

Lema. 33.5. (Lema corto de los cinco.)
Dado una diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_0 & \xrightarrow{f_0} & M_1 & \xrightarrow{f_1} & M_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle h_0} & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \\ 0 & \longrightarrow & N_0 & \xrightarrow{g_0} & N_1 & \xrightarrow{g_1} & N_2 & \longrightarrow & 0 \end{array}$$

Se verifica:

(1) Si h_0 y h_2 son inyectivos, también lo es h_1.
(2) Si h_0 y h_2 son sobreyectivos, también lo es h_1.
(3) Si h_0 y h_2 son isomorfismos, también lo es h_1.

DEMOSTRACIÓN. (1). Tenemos:

$$\begin{array}{ll} h_1(m_1) = 0 & \Rightarrow \\ g_1h_1(m_1) = 0 & \Rightarrow \\ h_2f_1(m_1) = 0 & \Rightarrow \\ f_1(m_1) = 0 & \Rightarrow \\ \exists m_0 \in M \text{ tal que } f_0(m_0) = m_1 & \Rightarrow \\ 0 = h_1(m_1) = h_1f_0(m_0) = g_0h_0(m_0) & \Rightarrow \\ m_0 = 0 & \Rightarrow \\ m_1 = f_0(m_0) = 0. & \end{array}$$

(2). Tenemos:

$$\begin{array}{ll}
n_1 \in N_1 & \Rightarrow \\
g_1(n_1) \in N_2 & \Rightarrow \\
\exists m_2 \in M_2 \text{ tal que } h_2(m_2) = g_1(n_1) & \Rightarrow \\
\exists m_1 \in M_1 \text{ tal que } f_1(m_1) = m_2 & \Rightarrow \\
\text{Los elementos } n_1, h_1(m_1) \in N_1 \text{ verifican:} & \\
\quad g_1(n_1 - h_1(m_1)) = g_1(n_1) - g_1h_1(m_1) = g_1(n_1) - h_2f_1(m_1) = g_1(n_1) - h_2(m_2) = 0 & \Rightarrow \\
\exists n_0 \in N_0 \text{ tal que } g_0(n_0) = n_1 - h_1(m_1) & \Rightarrow \\
\exists m_0 \in M_0 \text{ tal que } h_0(m_0) = n_0 & \Rightarrow \\
h_1(f_0(m_0) + m_1) = h_1f_0(m_0) + h_1(m_1) = g_0h_0(m_0) + h_1(m_1) & \\
\quad = n_1 - h_1(m_1) + h_1(m_1) = n_1. &
\end{array}$$

□

Una sucesión exacta corta $0 \to M_0 \stackrel{f_0}{\to} M_1 \stackrel{f_1}{\to} M_2 \to 0$ es **escindida** (a la izquierda) si existe un homomorfismo $g : M_2 \to M_1$ tal que $f_2 \circ g = \mathrm{id}_{M_2}$.

Dados dos A–módulos N y M una **extensión** de M por N es una sucesión exacta corta $\mathbb{E} := (0 \to N \to E \to M \to 0)$. Dos extensiones $\mathbb{E}_1$ y $\mathbb{E}_2$ de M por N son equivalentes si las sucesiones que definen son equivalentes, esto es, existe un diagrama conmutativo:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N & \longrightarrow & E_1 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{id}_N} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \mathrm{id}_M} & & \\
0 & \longrightarrow & N & \longrightarrow & E_2 & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Como consecuencia h ha de ser un isomorfismo. Una extensión se llama **escindida** si la sucesión exacta corta que define es escindida.

Dados dos A–módulos N y M, vamos a clasificar, salvo equivalencia, todas las extensiones escindidas de M por N.

En el caso que nos ocupa las sucesiones exactas cortas escindidas se pueden caracterizar de diversos modos.

Lema. 33.6.
Sea $0 \to M_0 \stackrel{f_0}{\to} M_1 \stackrel{f_1}{\to} M_2 \to 0$ una sucesión exacta. Son equivalentes:

(a) Existe $g : M_2 \to M_1$ tal que $f_1 \circ g = \mathrm{id}_{M_2}$, esto es, la sucesión escinde.
(b) Existe $f : M_1 \to M_0$ tal que $f \circ f_0 = \mathrm{id}_{M_0}$, esto es, la sucesión escinde a la derecha.
(c) Existe un homomorfismo $f : M_1 \to M_0 \oplus M_2$ tal que el siguiente diagrama conmuta.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_0 & \stackrel{f_0}{\longrightarrow} & M_1 & \stackrel{f_1}{\longrightarrow} & M_2 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle h_0} & & \downarrow{\scriptstyle h_1} & & \downarrow{\scriptstyle h_2} & & \\
0 & \longrightarrow & M_0 & \stackrel{incl.}{\longrightarrow} & M_0 \oplus M_2 & \stackrel{proy.}{\longrightarrow} & M_2 & \longrightarrow & 0
\end{array}$$

Corolario. 33.7.
Dados dos A–módulos N y M, toda extensión escindida de M por N es equivalente a una extensión definida por una suma directa, ver Ejemplo (33.2.).

Acabamos esta sección con algunos lemas técnicos sobre sucesiones exactas.

Proposición. 33.8.
(1) La sucesión $M_0 \stackrel{f_0}{\to} M_1 \stackrel{f_1}{\to} M_2 \to 0$ es exacta si, y solo si, para cualquier A–módulo M la sucesión

$$0 \longrightarrow \operatorname{Hom}_A(M_2,M) \xrightarrow{(f_1)^*} \operatorname{Hom}_A(M_1,M) \xrightarrow{(f_0)^*} \operatorname{Hom}_A(M_0,M)$$

es exacta.
(2) La sucesión $0 \to M_0 \stackrel{f_0}{\to} M_1 \stackrel{f_1}{\to} M_2$ es exacta si, y solo si, para cualquier A–módulo M la sucesión

$$0 \longrightarrow \operatorname{Hom}_A(M,M_0) \xrightarrow{(f_0)_*} \operatorname{Hom}_A(M,M_1) \xrightarrow{(f_0)_*} \operatorname{Hom}_A(M,M_2)$$

es exacta.

DEMOSTRACIÓN. Por dualidad basta hacer solo la primera parte. Supongamos que $M_0 \stackrel{f_0}{\to} M_1 \stackrel{f_1}{\to} M_2 \to 0$ es exacta, entonces para cada A–módulo M la sucesión del Hom es exacta.
(i). f_1^* es inyectiva. En efecto, si $g \in \operatorname{Hom}_A(M_2,M)$ verifica $f_1^*(g) = 0$, entonces $gf_1 = 0$, y como f_1 es sobreyectiva, tenemos $g = 0$.
(ii). $\operatorname{Im}(f_1^*) \subseteq \operatorname{Ker}(f_0^*)$; es consecuencia de que $f_0^* f_1^* = (f_1 f_0)^* = 0$.
(iii). $\operatorname{Ker}(f_0^*) \subseteq \operatorname{Im}(f_1^*)$; dado $g \in \operatorname{Ker}(f_0^*)$ tenemos $gf_0 = f_0^*(g) = 0$, luego existe $h : M_2 \longrightarrow M$ tal que $g = hf_1 = f_1^*(h)$ y $g \in \operatorname{Im}(f_1^*)$.

$$\begin{array}{ccccccc} M_0 & \xrightarrow{f_0} & M_1 & \xrightarrow{f_1} & M_2 & \longrightarrow & 0 \\ & & & g\searrow & \swarrow h & & \\ & & & & M & & \end{array}$$

La existencia de h es debida a que $M_2 \cong M_1/\operatorname{Ker}(f_1) = M_1/\operatorname{Im}(f_0)$ y a la propiedad universal del cociente.
Supongamos ahora que para cada A–módulo M la sucesión

$$0 \to \operatorname{Hom}_A(M_2,M) \stackrel{(f_1)^*}{\to} \operatorname{Hom}_A(M_1,M) \stackrel{(f_0)^*}{\to} \operatorname{Hom}_A(M_0,M)$$

es exacta.

(i). Vamos a ver que f_1 es simplificable a derecha, en efecto si $g \circ f_1 = 0$, entonces $f_1^*(g) = 0$, y como f_1^* es inyectiva, tenemos $g = 0$. Entonces f_1 es sobreyectiva.

(ii). $\operatorname{Im}(f_0) \subseteq \operatorname{Ker}(f_1)$. Basta ver que si $f : N \longrightarrow N'$ y para cada A–módulo M se tiene que $f^* : \operatorname{Hom}_A(N', M) \longrightarrow \operatorname{Hom}_A(N, M)$ es cero, entonces f es cero. Tomando $M = N'$ se tiene $0 = f^*(\mathrm{id}_{N'}) = \mathrm{id}_{N'} \circ f = f$. Ahora aplicando a este caso, como $0 = f_0^* \circ f_1^* = (f_1 \circ f_0)^*$, resulta $f_1 \circ f_0 = 0$.

(iii). Consideramos el siguiente diagrama

$$\begin{array}{ccccccc}
 & & & & M_1/\operatorname{Im}(f_0) & & \\
 & & & {\scriptstyle q}\nearrow & \;{\scriptstyle h}\searrow \nwarrow{\scriptstyle k} & & \\
M_0 & \xrightarrow{f_0} & M_1 & & \xrightarrow{f_1} & M_2 & \longrightarrow 0 \\
 & \searrow & \nearrow & & & & \\
 & \operatorname{Im}(f_0) & & & & &
\end{array}$$

h existe por la propiedad universal del cociente, y es única verificando $h \circ q = f_1$. Por otro lado ya que $\operatorname{Ker}(f_0^*) \subseteq \operatorname{Im}(f_1^*)$, al ser $0 = q \circ f_0 = f_0^*(q)$, existe k tal que $f_1^*(k) = q$, esto es, $q = k \circ f_1$; por ser f_1^* inyectivo k es único verificando esta condición. Ahora falta ver que h y k son mutuamente inversas. En efecto, $k \circ h \circ q = k \circ f_1 = q$, y como q es sobreyectiva se tiene $k \circ h = \mathrm{id}_{M_1/\operatorname{Im}(f_0)}$, y $h \circ k \circ f_1 = h \circ q = f_1$, y por ser f_1 sobreyectiva se tiene $h \circ k = \mathrm{id}_{M_2}$. Tenemos entonces que $\operatorname{Im}(f_0) = \operatorname{Ker}(f_1)$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Im}(f_0) & \longrightarrow & M_1 & \longrightarrow & M_1/\operatorname{Im}(f_0) & \longrightarrow & 0 \\
 & & \cong \downarrow & & \| & & \cong \downarrow h & & \\
0 & \longrightarrow & \operatorname{Ker}(f_1) & \longrightarrow & M_1 & \longrightarrow & M_1/\operatorname{Ker}(f_1) = M_2 & \longrightarrow & 0
\end{array}$$

□

Proposición. 33.9. (Lema de la serpiente.)
Para cualquier diagrama conmutativa con filas exactas

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M_0 & \xrightarrow{f_0} & M_1 & \xrightarrow{f_1} & M_2 & \longrightarrow & 0 \\
 & & {\scriptstyle h_0}\downarrow & & {\scriptstyle h_1}\downarrow & & {\scriptstyle h_2}\downarrow & & \\
0 & \longrightarrow & N_0 & \xrightarrow{g_0} & N_1 & \xrightarrow{g_1} & N_2 & \longrightarrow & 0
\end{array}$$

existe una sucesión exacta

$$0 \to \operatorname{Ker}(h_0) \stackrel{f_0'}{\to} \operatorname{Ker}(h_1) \stackrel{f_1'}{\to} \operatorname{Ker}(h_2) \stackrel{\Delta}{\to} \operatorname{Coker}(h_0) \stackrel{g_0'}{\to} \operatorname{Coker}(h_1) \stackrel{g_1'}{\to} \operatorname{Coker}(h_2) \to 0$$

donde $\operatorname{Coker}(h_i) = N_i/\operatorname{Im}(h_i)$ *y* f_0', f_1', g_0' *y* g_1' *son los homomorfismos inducidos por* f_0, f_1, g_0 *y* g_1.

DEMOSTRACIÓN. Consideramos el diagrama siguiente:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(h_0) & \xrightarrow{f'_0} & \mathrm{Ker}(h_1) & \xrightarrow{f'_1} & \mathrm{Ker}(h_2) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_0 & \xrightarrow{f_0} & M_1 & \xrightarrow{f_1} & M_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & \Delta & \downarrow & & \\
0 & \longrightarrow & N_0 & \xrightarrow{g_0} & N_1 & \xrightarrow{g_1} & N_2 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \dashrightarrow & \mathrm{Coker}(h_0) & \xrightarrow{g'_0} & \mathrm{Coker}(h_1) & \xrightarrow{g'_1} & \mathrm{Coker}(h_2) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Son inmediatas la exactitud de la sucesión $0 \longrightarrow \mathrm{Ker}(h_0) \xrightarrow{f'_0} \mathrm{Ker}(h_1) \xrightarrow{f'_1} \mathrm{Ker}(h_2)$ y la exactitud de la sucesión $\mathrm{Coker}(h_0) \xrightarrow{g'_0} \mathrm{Coker}(h_1) \xrightarrow{g'_1} \mathrm{Coker}(h_2) \longrightarrow 0$.

Para definir Δ tomamos $x \in \mathrm{Ker}(h_2)$. Existe $m_1 \in M_1$ tal que $f_1(m_1) = x$, entonces $g_1h_1(m_1) = h_2f_1(m_1) = h_2(x) = 0$, y existe un único $n_0 \in N_0$ tal que $g_0(n_0) = h_1(m_1)$. Definimos $\Delta(x) = n_0 + \mathrm{Im}(h_0)$.

Comprobamos que Δ está bien definida. En efecto, la elección de m_1 no es única, por lo que si tomamos otro m'_1 tal que $f_1(m'_1) = x$, llegamos a un n'_0. Vamos a ver que $n_0 - n'_0 \in \mathrm{Im}(h_0)$, y por tanto Δ está bien definida. Tenemos que $g_0(n'_0) = h_1(m'_1)$ y por otro lado $f_1(m_1) = x = f_1(m'_1)$, luego $m'_1 - m_1 \in \mathrm{Ker}(f_1) = \mathrm{Im}(f_0)$. Sea $m_0 \in M_0$ tal que $f_0(m_0) = m'_1 - m_1$. Se tiene

$$g_0(n'_0 - n_0) = h_1(m'_1 - m_1) = h_1f_0(m_0) = g_0h_0(m_0),$$

luego $n'_0 - n_0 = h_0(m_0)$ y tenemos el resultado.

Una vez que hemos comprobado que Δ está bien definida, veamos la exactitud en $\mathrm{Ker}(h_2)$. Para cada $m_1 \in \mathrm{Ker}(h_1)$ se tiene $\Delta f'_1(m_1) = n_0 + \mathrm{Im}(h_0)$, con $g_0(n_0) = h_1(m_1) = 0$. Por otro lado, si $x \in \mathrm{Ker}(\Delta)$, entonces $n_0 \in \mathrm{Im}(h_0)$, sea $n_0 = h_0(m_0)$, se tiene:

$$h_1(m_1) = g_0(n_0) = g_0 \circ h_0(m_0) = h_1 \circ f_0(m_0),$$

y $m_1 - f_0(m_0) \in \mathrm{Ker}(h_1)$. Por lo tanto

$$x = f_1(m_1) = f_1(m_1 - f_0(m_0)) = f'_1(m_1 - f_0(m_0)) \in \mathrm{Im}(f'_1).$$

Estudiamos la exactitud en $\operatorname{Coker}(h_0)$. Para cada $x \in \operatorname{Ker}(h_2)$ se tiene:

$$g_0'\Delta(x) = g_0'(n_0 + \operatorname{Im}(h_0)) = g_0(n_0) + \operatorname{Im}(h_1) = h_1(m_1) + \operatorname{Im}(h_1) = 0.$$

Por otro lado, si $n + \operatorname{Im}(h_0) \in \operatorname{Ker}(g_0')$, se tiene $g_0(n) \in \operatorname{Im}(h_1)$, y existe $x_1 \in M_1$ tal que $h_1(x_1) = g_0(n)$. Tenemos

$$h_2 \circ f_1(x_1) = g_1 \circ h_1(x_1) = g_1 \circ g_0(n) = 0,$$

esto es, $f_1(x_1) \in \operatorname{Ker}(h_2)$ y $\Delta(f_1(x_1)) = n + \operatorname{Im}(h_0)$. □

34. Ejercicios

Hom

Ejercicio. 34.1.
Dados A–módulos M_1, M_1, N_1, N_2, prueba que existe un isomorfismo

$$\mathrm{Hom}_A(M_1\oplus M_2, N_1\oplus N_2)\cong \mathrm{Hom}_A(M_1,N_1)\oplus \mathrm{Hom}_A(M_1,N_2)\oplus \mathrm{Hom}_A(M_2,N_1)\oplus \mathrm{Hom}_A(M_2,N_2).$$

Observa podemos escribir la suma directa

$$\mathrm{Hom}_A(M_1,N_1)\oplus \mathrm{Hom}_A(M_1,N_2)\oplus \mathrm{Hom}_A(M_2,N_1)\oplus \mathrm{Hom}_A(M_2,N_2)$$

como una matriz

$$\begin{pmatrix} \mathrm{Hom}_A(M_1,N_1) & \mathrm{Hom}_A(M_2,N_1) \\ \mathrm{Hom}_A(M_1,N_2) & \mathrm{Hom}_A(M_2,N_2) \end{pmatrix}$$

y este caso si tomamos $N_1 = M_1$ y $M_2 = N_2$, la composición en $\mathrm{Hom}_A(M_1\oplus M_2, N_1\oplus N_2)$ coincide con el producto de matrices.

SOLUCIÓN

Ejercicio. 34.2.
Si $\{N_i \mid i\in I\}$ es una familia de A–módulos, para cada A–módulo M prueba que existe un isomorfismo

$$\mathrm{Hom}_A(M,\prod_i N_i)\cong \prod_i \mathrm{Hom}_A(M,N_i).$$

Ver también el ejercicio (29.8.). *SOLUCIÓN*

Ejercicio. 34.3.
Si $\{M_i \mid i\in I\}$ es una familia de A–módulos, para cada A–módulo N prueba que existe un isomorfismo

$$\mathrm{Hom}_A(\oplus_i M_i, N)\cong \prod_i \mathrm{Hom}_A(M,N_i).$$

Ver también el ejercicio (29.8.). *SOLUCIÓN*

Ejercicio. 34.4.
Se consideran los grupos abelianos $A = \mathbb{Z}_2 \oplus \mathbb{Z}_4$ *y* $B = \mathbb{Z}_4 \oplus \mathbb{Z}_{12}$. *Determinar la estructura del grupo abeliano* $\operatorname{Hom}(A, B)$.

SOLUCIÓN

Ejercicio. 34.5.
Estudia los siguientes enunciados:
(1) Determina el grupo abeliano $\operatorname{Hom}(\mathbb{Z}_{15}, \mathbb{Z}_{36})$, *y haz un listado de sus elementos.*
(2) Para enteros positivos n *y* m, *determina el grupo abeliano* $\operatorname{Hom}(\mathbb{Z}_n, \mathbb{Z}_m$, *prueba que es isomorfo a* $\mathbb{Z}_d$, *donde* $d = \mathrm{m.c.d.}\{n, m\}$.

Ver también el ejercicio (29.9.). SOLUCIÓN

Sucesiones exactas

Ejercicio. 34.6.
La sucesión $0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2$ *es exacta si, y solosi, para cualquier* A*–módulo* M *la sucesión*

$$0 \to \operatorname{Hom}_A(M, M_0) \xrightarrow{(f_0)_*} \operatorname{Hom}_A(M, M_1) \xrightarrow{(f_1)_*} \operatorname{Hom}_A(M, M_2)$$

es exacta.

SOLUCIÓN

Ejercicio. 34.7.
Da un ejemplo de una sucesión exacta corta$0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \to 0$ *y un* A*–módulo* M *paralos que en la sucesión exacta*

$$0 \to \operatorname{Hom}_A(M, M_0) \xrightarrow{(f_0)_*} \operatorname{Hom}_A(M, M_1) \xrightarrow{(f_1)_*} \operatorname{Hom}_A(M, M_2)$$

el homomorfismo $(f_1)^*$ *no sea sobreyectivo.*

SOLUCIÓN

Ejercicio. 34.8.
Haz una demostración de que en una sucesión exacta corta de A–módulos $0 \to M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \to 0$ *son equivalentes:*

(a) *Existe un homomorfismo* $g : M_2 \to M_1$ *tal que* $f_1 \circ g = \mathrm{id}_{M_2}$.
(b) *Existe un homomorfismo* $f : M_1 \to M_0$ *tal que* $f \circ f_0 = \mathrm{id}_{M_0}$.

SOLUCIÓN

Ejercicio. 34.9.
Prueba que la ley modular: si $N_1, N_2, K \subseteq M$ *son submódulos de un módulo* M *tales que* $N_1 \subseteq N_2$,*entonces* $N_1 + (K \cap N_2) = (N_1 + K) \cap N_2$, *es equivalente a la exactitud de la sucesión*

$$0 \to \frac{K \cap N_2}{K \cap N_1} \to \frac{N_2}{N_1} \to \frac{K + N_2}{K + N_1} \to 0.$$

(Con las identificaciones necesarias.)

SOLUCIÓN

Productos

Ejercicio. 34.10.
Dado un anillo sin uno B *podemos construir un anillo con uno,* B_1*, del cual* B *es un ideal en la siguiente forma:En el producto cartesiano* $B \times \mathbb{Z}$ *definimos dos operaciones:*

$$\begin{aligned}(b_1, n_1) + (b_2, n_2) &= (b_1 + b_2, n_1 + n_2),\\ (b_1, n_1) \cdot (b_2, n_2) &= (b_1 b_2 + b_1 n_2 + b_2 n_2, n_1 n_2),\end{aligned}$$

para cualesquiera $b_1, b_2 \in B$ *y* $n_1, n_2 \in \mathbb{Z}$.

(1) *Prueba que* $B_1 = B \times \mathbb{Z}$ *es un anillo con elemento uno igual a* $(0,1)$.
(2) ***Propiedad universal.****Prueba que para cada anillo (con uno)* A *y cada aplicación* $g : B \longrightarrow A$, *que sea homomorfismo para la suma y el producto, existe un único homomorfismo de anillos* $g' : B_1 = B \times \mathbb{Z} \longrightarrow A$ *tal que* $g'_{|B} = g$ *cuando identificamos* B *son* $B \times 0 \subseteq B \times \mathbb{Z}$.
(3) *Tomando* $g = 0$ *tenemos que* $B = \mathrm{Ker}(0)$, *y por tanto* B *es un ideal de* $B_1 = B \times \mathbb{Z}$.

El anillo $B_1 = B \times \mathbb{Z}$ *se llama la* **extensión de Dorroh** *de* B.

SOLUCIÓN

Ejercicio. 34.11.
Sea K un cuerpo y V un espacio vectorial sobre K. En $K \times V$ se define la suma componente a componente y la multiplicación mediante

$$(k_1, v_1)(k_2, v_2) = (k_1k_2, k_1v_2 + k_2v_1).$$

(1) Prueba que con $1 = (1, 0)$, el conjunto $K \times V$ es un anillo. Se llama la **extensión trivial** *de K por V, y se representa por $K \ltimes V$.*
(2) Prueba que $j : K \to K \ltimes V$, $j(k) = (k, 0)$ es un homomorfismo de anillos.
(3) Prueba que $W = \{(0, v) \mid v \in V\} \subseteq K \ltimes V$ es un ideal que verifica $W^2 = 0$ y que es el núcleo de la aplicación $p : K \ltimes V \to K$ definida $p(k, v) = k$.
(4) Prueba que $p \circ j = id_K$:

$$\begin{array}{ccccc} & & & & K \\ & & & \swarrow^{j} & \downarrow id \\ W & \xrightarrow{i} & K \ltimes V & \xrightarrow{p} & K \end{array}$$

SOLUCIÓN

Ejercicio. 34.12.
Sea A un anillo y M un A–módulo. La extensión trivial de A por M se define como $A \ltimes M = A \times M$ con multiplicación $(a_1, m_1)(a_2, m_2) = (a_1a_2, a_1m_2 + a_2m_1)$ y elemento uno igual a $(1, 0)$.
(1) Determina los ideales primos de $A \ltimes M$ en función de los ideales primos de A.
(2) ¿Son isomorfos $\mathbb{Z}_2 \times \mathbb{Z}_2$ y $\mathbb{Z}_2 \ltimes \mathbb{Z}_2$?

SOLUCIÓN

Subanillos

Ejercicio. 34.13.
Dado un anillo A y un elemento $b \in A$, consideramos el conjunto

$$B = \{bF(b) + n \cdot 1 \mid F \in \mathbb{Z}[X],\ n \in \mathbb{Z}\}.$$

Prueba que B es un anillo.

SOLUCIÓN

Homomorfismos

Ejercicio. 34.14.
Prueba que cada monomorfismo de anillos (= homomorfismo de anillos simplificable a izquierda) $f : A \longrightarrow C$ es una aplicación inyectiva.

SOLUCIÓN

Ejercicio. 34.15.
Prueba que la inclusión $\mathbb{Z} \to \mathbb{Q}$ es un epimorfismo de anillos (= homomorfismo de anillos simplificable a derecha), y que por tanto los epimorfismos no son necesariamente aplicaciones sobreyectivas.

SOLUCIÓN

Producto tensor

Ejercicio. 34.16.
Sea M un grupo abeliano y $n \in \mathbb{N}$, $n \geq 2$. Se define $nM = \{nm \mid \ m \in M\}$. Prueba que se tiene un isomorfismo

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} M \cong \frac{M}{nM}.$$

SOLUCIÓN

Ejercicio. 34.17.
Dados $n, m \in \mathbb{N}$, $n, m \geq 2$, si $h = \mathrm{m.c.d.}\{n, m\}$, prueba que se tiene

$$\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \mathbb{Z}_h.$$

SOLUCIÓN

Ejercicio. 34.18.
Un grupo abeliano M se llama de **torsion** *si cada elemento de M tiene orden finito, y es* **divisible** *si $M = nM$ para todo $n \in \mathbb{N}$.*

(1) Prueba que si M ó N es torsión, entonces $M \otimes_{\mathbb{Z}} N$ es torsión.
(2) Prueba que si M o N es divisible, entonces $M \otimes_{\mathbb{Z}} N$ es divisible.
(3) Prueba que si M es torsión y N es divisible, entonces $M \otimes_{\mathbb{Z}} N = 0$.

SOLUCIÓN

Ejercicio. 34.19.
Dada una familia de A–módulos $\{M_i \mid i \in I\}$. Prueba que para cada A–módulo N se tiene

$$(\oplus_i M_i) \otimes_A N \cong \oplus_i (M_i \otimes_A N).$$

SOLUCIÓN

Capítulo VI

Dependencia entera

Introducción

En este capítulo vamos a establecer los resultados más importantes de la teoría que relaciona los conjuntos algebraicos con las álgebras sobre cuerpos: aquellos que tratan de la dimensión. La primera sección está dedicada al estudio de la dependencia entera y las extensiones enteras, probando los resultados que relacionan las cadenas de ideales primos en extensiones enteras de anillos. En la segunda se prueba el Teorema de Normalización de Noether y sus consecuencias, y en la tercera el Teorema de los ceros de Hilbert, que establece una biyección entre conjuntos algebraicos en $\mathbb{A}^n(K)$ e ideales radicales del anillo $K[X_1, \ldots, X_n]$, cuando K es un cuerpo algebraicamente cerrado. Finaliza el capítulo recordando los resultados sobre extensiones trascendentes que son de aplicación en esta teoría.

35. Extensiones enteras

Dependencia entera

Sea $A \subseteq B$ una extensión de anillos. Un elemento $x \in B$ se llama **entero** sobre A si existe un polinomio mónico $F \in A[X]$ tal que $F(x) = 0$.

Teorema. 35.1.
Sea $A \subseteq B$ una extensión de anillos y $x \in B$ un elemento. Son equivalentes:
(a) x es entero sobre A;
(b) $A[x]$ es un A–módulo finitamente generado;
(c) $A[x]$ está contenido en un subanillo $A \subseteq C \subseteq B$ que es un A–módulo finitamente generado;
(d) Existe un $A[x]$–módulo fiel finitamente generado M que es un A–módulo finitamente generado.

DEMOSTRACIÓN. (a)⇒(b). Si $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, con $a_i \in A$, entonces $x^n = -(a_{n-1}x^{n-1} + \cdots + a_0)$ y por inducción probamos que $x^{n+h} \in A + Ax + \cdots + Ax^{n-1}$, entonces $A[x]$ es un A–módulo finitamente generado.

(b)⇒(c). Tomamos $C = A[x]$.

(c)⇒(d). Podemos tomar $M = C$, ya que por ser $A[x] \subseteq C$, resulta que C es un $A[x]$–módulo, y por ser $1 \in C$ es fiel. Además, por hipótesis, C es un A–módulo finitamente generado.

(d)⇒(a). Sea M un $A[x]$–módulo fiel y finitamente generado como A–módulo, entonces podemos definir un endomorfismo $\lambda_x \colon M \to M$ mediante $\lambda_x(m) = xm$, para cada $m \in M$. Sea $\{x_1, \ldots, x_t\}$ un sistema de generadores de M, y supongamos que

$$\lambda_x(m_i) = \sum_{j=1}^{t} a_{ij}m_j,$$

entonces $xm_i = \sum_{j=1}^{t} a_{ij}m_j$ y de aquí obtenemos la igualdad de matrices

$$(x\ \mathrm{id} - (a_{ij})_{ij})(m_i)_i = 0,$$

de donde deducimos que $\det(x\ \mathrm{id} - (a_{ij})_{ij})(m_i)_i = 0$. Y por tanto $\det(x\ \mathrm{id} - (a_{ij})_{ij}) \in \mathrm{Ann}(M) = 0$. Ahora bien, desarrollando $\det(x\ \mathrm{id} - (a_{ij})_{ij})$ se obtiene una expresión de la forma:

$$x^t + a_{t-1}x^{t-1} + \cdots + a_1x + a_0 = 0, \text{ con } a_i \in A,$$

luego x es un elemento entero sobre A. □

Corolario. 35.2.
Sea $A \subseteq B$ una extensión de anillos y $x_1, \ldots, x_t \in B$ elementos de B enteros sobre A, entonces el anillo $A[x_1, \ldots, x_t]$ es un A–módulo finitamente generado.

DEMOSTRACIÓN. Basta hacer inducción sobre t, ya que para cada índice $i \leq t$ se verifica que x_i es entero sobre $A[x_1, \ldots, x_{i-1}]$. □

Corolario. 35.3.
Sea $A \subseteq B$ una extensión de anillos, el conjunto C de todos los elementos de B enteros sobre A es un subanillo de B que contiene a A.

DEMOSTRACIÓN. Es claro que cada elemento $a \in A$ es entero sobre A, por tanto $A \subseteq C$. Si $x, y \in C$, entonces $x + y \in A[x, y]$ y como $A[x, y]$ es un A–módulo finitamente generado, resulta que $x + y$ es entero. Para xy se hace igual. □

Con la notación del Corolario anterior el subanillo C se llama la **clausura entera** de A en B. El anillo A se llama **íntegramente cerrado en** B si $A = C$. Cuando $B = C$, se dice que B es **entero** sobre A.

Un dominio A se llama **normal** o **íntegramente cerrado** si es íntegramente cerrado en su cuerpo de fracciones. Dado un dominio A su clausura entera en el cuerpo de fracciones se llama la **normalización** de A.

Ejemplo. 35.4.
Si K y L son cuerpos, $K \subseteq L$, entonces K/L es una extensión algebraica si y solo si $K \subseteq L$ es una extensión entera.

Ejercicio. 35.5.
$\mathbb{Z}$ es un dominio normal. Ver también Teorema (35.6.).

DEMOSTRACIÓN. Sea $r/s \in \mathbb{Q}$, una fracción irreducible, entero sobre $\mathbb{Z}$, entonces existen $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$ tales que $(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$, y por tanto obtenemos una expresión de la forma:

$$r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n = 0,$$

luego s divide a r^n, lo que es una contradicción salvo que $s = 1$, y en este caso $r/s \in \mathbb{Z}$. □

La prueba de que $\mathbb{Z}$ es un anillo normal se puede extender a cualquier dominio de factorización única.

Teorema. 35.6.
Cada dominio de factorización única es un dominio normal.

DEMOSTRACIÓN. Igual demostración que en el Ejercicio (35.5.). □

Ejemplo. 35.7.
Sea K un cuerpo y $A = K[X,Y]$. El ideal $\mathfrak{a} = (X^2 - Y^3)$ es primo, y por tanto $A/\mathfrak{a}$ es un dominio. Se verifica que $A/\mathfrak{a}$ no es normal.
En efecto, el elemento $x = \overline{X}/\overline{Y}$ del cuerpo de fracciones de $A/\mathfrak{a}$ es entero sobre $A/\mathfrak{a}$, ya que es raíz del polinomio $X^2 - \overline{Y}$, y no pertenece a $A/\mathfrak{a}$.

Corolario. 35.8. (Transitividad de las extensiones enteras.)
Se considera $A \subseteq B_1 \subseteq B_2$ una cadena de extensiones de anillos, siendo B_1 entero sobre A y B_2 entero sobre B_1, entonces B_2 es entero sobre A.

DEMOSTRACIÓN. Sea $x \in B_2$, existen $b_{n-1},\ldots,b_0 \in B_1$ tales que $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$. Llamamos $A' = A[b_0,\ldots,b_{n-1}]$, se verifica que x es entero sobre A', luego $A[b_0,\ldots,b_{n-1},x]$ es un A'–módulo finitamente generado, y como consecuencia es un A–módulo finitamente generado, entonces x es entero sobre A. □

Corolario. 35.9.
Sea $A \subseteq B$ una extensión de anillos y C la clausura entera de A en B, entonces C es íntegramente cerrado en B.

DEMOSTRACIÓN. Llamemos C' a la clausura entera de C en B, entonces

$$A \subseteq C \subseteq C'$$

son extensiones enteras, luego $A \subseteq C'$ es una extensión entera y se verifica $C' \subseteq C$. □

Ejercicio. 35.10.
Sea A un dominio con cuerpo de fracciones K y sea $K \subseteq L$ una extensión de cuerpos. Si $x \in L$ es algebraico sobre K, entonces existe $a \in A$ tal que $0 \neq ax$ es entero sobre A.

SOLUCIÓN. Sea $0 \neq F \in K[X]$ un polinomio tal que $F(x) = 0$. Multiplicando F por el producto de los denominadores de los coeficientes de F podemos obtener un polinomio $0 \neq rF \in A[X]$ tal que $rF(x) = 0$. Si $rF = aX^n + a_{n-1}X^{n-1} + \cdots + a_0$, entonces multiplicando por a^{n-1}, tenemos

$$(ax)^n + a_{n-1}(ax)^{n-1} + \cdots + a_1a^{n-1}(ax) + a_0a^{n-1} = 0,$$

y ax es entero sobre A. □

Proposición. 35.11.
Sea $A \subseteq B$ es una extensión entera de anillos y $\mathfrak{b} \subseteq B$ es un ideal de B. Si definimos $\mathfrak{a} = \mathfrak{b} \cap A$, entonces $A/\mathfrak{a} \subseteq B/\mathfrak{b}$ es una extensión entera.

DEMOSTRACIÓN. Es pasar una expresión del tipo $s^n + a_{n-1}s^{n-1} + \cdots + a_0$ de B a $B/\mathfrak{b}$. □

Ideales primos en extensiones enteras

Vamos a estudiar los ideales primos y maximales en extensiones enteras.

Proposición. 35.12.
Sea $A \subseteq B$ una extensión de dominios de integridad, siendo B entero sobre A. Son equivalentes:
(a) B es un cuerpo;
(b) A es un cuerpo.

DEMOSTRACIÓN. (a)⇒(b). Si B es un cuerpo y $0 \neq x \in A$, entonces existe $x^{-1} \in B$ que es entero sobre A, luego existe una expresión del tipo

$$x^{-n} + a_{n-1}x^{-n+1} + \cdots + a_0 = 0.$$

Multiplicando por x^{n-1} obtenemos:

$$x^{-1} + a_{n-1} + \cdots + a_0x^{n-1} = 0,$$

y de aquí

$$x^{-1} = -(a_{n-1} + \cdots + a_0x^{n-1}) \in A.$$

(b)⇒(a). Si A es un cuerpo y $0 \neq x \in B$, existe una expresión del tipo

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

supongamos que n es el menor de los posibles enteros verificando lo anterior. Por ser B un dominio de integridad se verifica $a_0 \neq 0$ y podemos construir la expresión $x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) = -a_0$, luego

$$x^{-1} = -a_0^{-1}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1).$$

□

Corolario. 35.13.
Sea $A \subseteq B$ una extensión entera de anillos y sea $\mathfrak{q} \subseteq B$ un ideal primo. Llamamos $\mathfrak{p} = \mathfrak{q} \cap A$. Son equivalentes:

(a) $\mathfrak{q}$ es maximal;
(b) $\mathfrak{p}$ es maximal.

DEMOSTRACIÓN. Tenemos que $A/\mathfrak{p} \subseteq B/\mathfrak{q}$ es una extensión de anillos y $B/\mathfrak{q}$ es entero sobre $A/\mathfrak{p}$. Además, como $B/\mathfrak{q}$ es un dominio de integridad, resulta que $B/\mathfrak{q}$ es un cuerpo si, y sólo si, $A/\mathfrak{p}$ es un cuerpo y entonces $\mathfrak{q}$ es un ideal maximal de B si, y sólo si, $\mathfrak{p}$ es un ideal maximal. □

Lema. 35.14.
Sea $A \subseteq B$ una extensión entera de anillos y $\mathfrak{p} \subseteq A$ un ideal primo. Existe un ideal primo $\mathfrak{q} \subseteq B$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$.

DEMOSTRACIÓN. Llamamos $\Sigma = A \setminus \mathfrak{p}$ y $\Gamma = \{\mathfrak{a} \subseteq B \mid \ \mathfrak{a} \cap \Sigma = \varnothing\}$. Como Γ es inductivo existen elementos maximales en Γ; cada elemento maximal de Γ es un ideal primo de B. Dado $\mathfrak{q} \in \Gamma$ maximal tenemos que $\mathfrak{q} \cap A \subseteq \mathfrak{p}$; para probar la otra inclusión, sea $a \in \mathfrak{p} \setminus (\mathfrak{q} \cap A)$. Como $\mathfrak{q} \subset (\mathfrak{q}, a)$, entonces existe $s \in (\mathfrak{q}, a) \cap \Sigma$; escribimos $s = q + ba$, con $q \in \mathfrak{q}$ y $b \in B$.

Al ser b entero sobre A existe una combinación $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$ con $a_i \in A$. Multiplicando por a^n tenemos:

$$(ba)^n + a_{n-1}a(ba)^{n-1} + \cdots + a_0a^n = 0.$$

De la relación $s - q = ab$ se deduce que

$$y := s^n + a_{n-1}as^{n-1} + \cdots + a_0a^n \equiv 0 \pmod{\mathfrak{q}},$$

y tenemos $y \in \mathfrak{q} \cap A \subseteq \mathfrak{p}$; como $a \in \mathfrak{p}$, se sigue $s \in \mathfrak{p}$, lo que es una contradicción. □

Teorema. 35.15. (Teorema del ascenso.)
Sea $A \subseteq B$ una extensión entera de anillos, $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ una cadena ascendente de ideales primos de A y $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ una cadena ascendente de ideales primos de B verificando $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $1 \leq i \leq m < n$.

$$\begin{array}{l} \mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots \subseteq \mathfrak{p}_m \subseteq \cdots \subseteq \mathfrak{p}_n \\ \mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \cdots \subseteq \mathfrak{q}_m \end{array}$$

Entonces la cadena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ se puede extender a una cadena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m \subseteq \cdots \subseteq \mathfrak{q}_n$ en la que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$, para $1 \leq i \leq n$.

DEMOSTRACIÓN. Podemos suponer que $m = 1$ y $n = 2$ y posteriormente hacer inducción. De la extensión entera $A \subseteq B$ pasamos a la extensión $A/\mathfrak{p}_1 \subseteq B/\mathfrak{q}_1$, que también es entera. En $A/\mathfrak{p}_1$ tenemos un ideal primo $\mathfrak{p}_2/\mathfrak{p}_1$, por lo que para reducir supondremos que tenemos una extensión entera de dominios $A \subseteq B$ y un ideal primo $\mathfrak{p} \subseteq A$. Aplicando el Lema (35.14.) existe un ideal $\mathfrak{q} \subseteq B$ tal que $\mathfrak{q} \cap A = \mathfrak{p}$. □

Dada una extensión entera de anillos $A \subseteq B$ y un ideal primo $\mathfrak{p} \subseteq A$, es posible que existan varios ideales primos $\mathfrak{q}_1, \mathfrak{q}_2 \subseteq B$ tales que $\mathfrak{q}_1 \cap A = \mathfrak{p} = \mathfrak{q}_2 \cap B$. Veamos un ejemplo:

Ejemplo. 35.16.
Tomamos $A = \mathbb{R}[X]$, $B = \mathbb{C}[X]$, $\mathfrak{p} = (X^2+1)\mathbb{R}[X]$, $\mathfrak{q}_1 = (X+i)\mathbb{C}[X]$, $\mathfrak{q}_2 = (X-i)\mathbb{C}[X]$. Se verifica:

$$(X+i)\mathbb{C}[X] \cap \mathbb{R}[X] = (X^2+1)\mathbb{R}[X] = (X-i)\mathbb{C}[X] \cap \mathbb{R}[X].$$

$$\begin{array}{lccc} \mathbb{C}[X]: & \mathfrak{q}_1 = (X+i)\mathbb{C}[X] & & \mathfrak{q}_2 = (X-i)\mathbb{C}[X] \\ & \searrow & & \swarrow \\ \mathbb{R}[X]: & & \mathfrak{p} = (X^2+1)\mathbb{R}[X] & \end{array}$$

En estas circunstancias vamos a comprobar que siempre los ideales de B que tienen la misma traza en A son incomparables.

Teorema. 35.17. (Teorema de incomparabilidad.)
Sea $A \subseteq B$ una extensión entera de anillos y $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ ideales de B tales que $\mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A$, entonces $\mathfrak{q}_1 = \mathfrak{q}_2$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{q}_1 \subsetneqq \mathfrak{q}_2$ y sea $b \in \mathfrak{q}_2 \setminus \mathfrak{q}_1$. Como b es entero sobre A tomamos $n \geq 1$ mínimo tal que existe una combinación verificando:

$$b^n + a_{n-1}b^{n-1} + \cdots + a_0 \equiv 0 \pmod{\mathfrak{q}_1}.$$

Como $b \notin \mathfrak{q}_1$ se tiene $n > 1$ y $a_0 \in \mathfrak{q}_2$, luego $a_0 \in \mathfrak{q}_2 \cap A = \mathfrak{q}_1 \cap A$, y tenemos

$$b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) \in \mathfrak{q}_1,$$

y como $b \notin \mathfrak{q}_1$, y $\mathfrak{p}$ es primo, tenemos una contradicción con la minimalidad de n. □

Dominios normales. Teorema del descenso

Sea $A \subseteq B$ una extensión de anillos y sea $\mathfrak{a}$ un ideal de A. Un elemento $x \in B$ se llama **entero sobre el ideal** $\mathfrak{a}$ si verifica una relación de dependencia entera,

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

con los $a_i \in \mathfrak{a}$.

Llamamos **clausura entera en** B **de un ideal** $\mathfrak{a}$ **de** A al conjunto de todos los elementos de B enteros sobre $\mathfrak{a}$.

Lema. 35.18.
Sea $A \subseteq B$ una extensión de anillos y $\mathfrak{a}$ un ideal de A. Si $A \subseteq C \subseteq B$ es la clausura entera de A en B, entonces la clausura entera de $\mathfrak{a}$ en B es el radical de $\mathfrak{a}C$ en C.

DEMOSTRACIÓN. Sea $x \in B$ un elemento entero sobre $\mathfrak{a}$; existen $a_i \in \mathfrak{a}$ tales que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Entonces $x \in C$ y como

$$x^n = -(a_{n-1}x^{n-1} + \cdots + a_0) \in \mathfrak{a}C,$$

tenemos que $x \in \operatorname{rad}(\mathfrak{a}C)$. Para ver la otra inclusión, sea $x \in \operatorname{rad}(\mathfrak{a}C)$, entonces existe n tal que $x^n = \sum_{j=1}^{m} a_j t_j$, con $a_j \in \mathfrak{a}$ y $t_j \in C$. Ya que cada a_j es entero sobre A, tenemos que $M = A[a_1, \ldots, a_m]$ es un A–módulo finitamente generado. Además se verifica $x^n M \subseteq \mathfrak{a}M$. Aplicando el Lema de Cayley-Hamilton (para la multiplicación por x^n), Lema (27.1.), tenemos que x^n es entero sobre $\mathfrak{a}$, en consecuencia x es entero sobre $\mathfrak{a}$. □

Proposición. 35.19.
Sea $A \subseteq B$ una extensión de dominios de integridad con A normal. Sea $x \in B$ un elemento entero sobre un ideal $\mathfrak{a} \subseteq A$. Entonces x es algebraico sobre K, el cuerpo de fracciones de A, y su polinomio minimal sobre K es

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

con $a_i \in \operatorname{rad}(\mathfrak{a})$.

DEMOSTRACIÓN. Tenemos que x es algebraico sobre K. Llamemos L al cuerpo de descomposición del polinomio irreducible $\operatorname{Irr}(x,K)$ de x sobre K, y sean $x_1,\dots,x_n$ todos los conjugados de x. Como cada x_i verifica la misma relación de dependencia que x, tenemos que todos son enteros sobre $\mathfrak{a}$. Los coeficientes de $\operatorname{Irr}(x,K)$ son polinomios en los x_i, y por tanto son elementos de K enteros sobre $\mathfrak{a}$. Ahora, como A es normal, la clausura entera de $\mathfrak{a}$ en K es $\operatorname{rad}(\mathfrak{a})$, luego todos pertenecen a $\operatorname{rad}(\mathfrak{a})$. □

Teorema. 35.20. (Teorema del descenso.)
Sea $A\subseteq B$ una extensión entera de dominios de integridad con A normal. Sean $\mathfrak{p}_1\supseteq\cdots\supseteq\mathfrak{p}_n$ una cadena de ideales primos de A y $\mathfrak{q}_1\supseteq\cdots\supseteq\mathfrak{q}_m$ una cadena de ideales primos de B verificando: $\mathfrak{q}_i\cap A=\mathfrak{p}_i$, $1\leq i\leq m<n$.

$$\begin{array}{l}\mathfrak{p}_1\supseteq\mathfrak{p}_2\supseteq\cdots\supseteq\mathfrak{p}_m\supseteq\cdots\supseteq\mathfrak{p}_n\\ \mathfrak{q}_1\supseteq\mathfrak{q}_2\supseteq\cdots\supseteq\mathfrak{q}_m\end{array}$$

Entonces la cadena $\mathfrak{q}_1\supseteq\cdots\supseteq\mathfrak{q}_m$ se puede extender a una cadena $\mathfrak{q}_1\supseteq\cdots\supseteq\mathfrak{q}_m\supseteq\cdots\supseteq\mathfrak{q}_n$ verificando: $\mathfrak{q}_i\cap A=\mathfrak{p}_i$, para $1\leq i\leq n$.

DEMOSTRACIÓN. (Necesitamos localización.) Vamos a suponer que $n=2$ y $m=1$ y después podremos hacer inducción. Localizamos B en $\mathfrak{q}_1$ y tenemos una cadena de extensiones

$$A\subseteq B\subseteq B_{\mathfrak{q}_1}.$$

Para ver que existe un ideal primo $\mathfrak{q}_2\subseteq B$ tal que $\mathfrak{q}_2\cap A=\mathfrak{p}_2$, basta ver que $\mathfrak{p}_2B_{\mathfrak{q}_1}\cap A=\mathfrak{p}_2$.
Dado un elemento de $y/s\in\mathfrak{p}_2B_{\mathfrak{q}_1}$, con $y\in\mathfrak{p}_2B\subseteq\operatorname{rad}(\mathfrak{p}_2B)$, tenemos que y es entero sobre $\mathfrak{p}_2$ y si el polinomio minimal de y sobre K, el cuerpo de fracciones de A, es

$$X^n+a_{n-1}X^{n-1}+\cdots+a_0,$$

entonces tiene sus coeficientes en $\mathfrak{p}_2$.
Dado $x\in\mathfrak{p}_2B_{\mathfrak{q}_1}\cap A$, sea $x=y/s$, entonces $s=yx^{-1}$ en K. El polinomio minimal de s sobre K se obtiene del anterior en la siguiente forma:

$$X^n+(a_{n-1}/x)X^{n-1}+\cdots+(a_0/x^n), \tag{VI.1}$$

Como $s\in B\setminus\mathfrak{q}_1$ es entero sobre A, entonces cada coeficiente a_i/x^{n-1} pertenece a A. (Aplicar la Proposición (35.19.) al ideal $\mathfrak{a}=A$.) Si $x\notin\mathfrak{p}_2$, entonces cada coeficiente $a_i/x^{n-i}\in\mathfrak{p}_2$ ya que $x^{n-j}(a_j/x^{n-j})=a_j\in\mathfrak{p}_2$ y $\mathfrak{p}_2$ es un ideal primo. Como s verifica la relación (VI.1), tenemos que

$$s^n\in\mathfrak{p}_2B\subseteq\mathfrak{p}_1B\subseteq\mathfrak{q}_1,$$

lo que es una contradicción. Tenemos entonces $x\in\mathfrak{p}_2$ y por tanto $\mathfrak{p}_2B_{\mathfrak{q}_2}\cap A\subseteq\mathfrak{p}_2$. La otra inclusión es clara y tenemos la igualdad. □

36. Lema de normalización de Noether

Dimensión de Krull de un anillo

Sea A un anillo (conmutativo). Una cadena de ideales primos

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$$

se dice que tiene **longitud** n. Se define la **dimensión** del anillo A como el supremo de las longitudes de las cadenas de ideales primos de A, y se representa por $\dim(A)$.

Si $\mathfrak{p}$ es un ideal primo de A, se define la **altura** de $\mathfrak{p}$ como el supremo de las longitudes de las cadenas de ideales primos del siguiente tipo:

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n = \mathfrak{p}.$$

La altura del ideal $\mathfrak{p}$ se representa por $\mathrm{ht}(\mathfrak{p})$.

Si $\mathfrak{a}$ es un ideal de A, se define la **altura** de $\mathfrak{a}$ como el mínimo de las alturas de los ideales primos minimales conteniendo a $\mathfrak{a}$. La altura del ideal $\mathfrak{a}$ se representa por $\mathrm{ht}(\mathfrak{a})$.

Los resultados sobre extensiones enteras de anillos nos dan la siguiente relación para las dimensiones de anillos.

Proposición. 36.1.
Sea $A \subseteq B$ una extensión entera de anillos. Si $\dim(A)$ es finita, entonces se verifica:

$$\dim(A) = \dim(B).$$

Ejercicio. 36.2.
Sea A un anillo y $\mathfrak{a}$ un ideal de A. Existe un isomorfismo de anillos

$$(A/\mathfrak{a})[X] \cong A[X]/\mathfrak{a}[X]$$

Como consecuencia:

(1) Si $\mathfrak{p} \subseteq A$ es un ideal primo, entonces $\mathfrak{p}[X]$ es un ideal primo de $A[X]$
(2) Si $\mathfrak{a} \subsetneqq \mathfrak{b}$ son ideales de A, entonces $\mathfrak{a}[X] \subsetneqq \mathfrak{b}[X]$.

Lema. 36.3.
Sea K un cuerpo y $X_1,\ldots,X_n$ indeterminadas sobre K, entonces tenemos una cadena ascendente

$$0\subset(X_1)\subset(X_1,X_2)\subset\cdots\subset(X_1,\cdots,X_n),$$

en la que todos son ideales primos y por tanto siempre se verifica: $\dim(K[X_1,\ldots,X_n])\geq n$.

Podemos completar este resultado para obtener la igualdad.

Teorema. 36.4.
Sea K un cuerpo y $X_1,\ldots,X_n$ indeterminadas sobre K, se tiene $\dim(K[X_1,\ldots,X_n])=n$.

DEMOSTRACIÓN. Sólo tenemos que probar la relación $\dim(K[X_1,\ldots,X_n])\leq n$.
Observa que $K[X_1,\ldots,X_n]$ tiene como máximo n elementos algebraicamente independientes, esto lo podemos razonar pasando al cuerpo de fracciones $K(X_1,\ldots,X_n)$ y viendo que el máximo número de elementos de un conjunto algebraicamente independiente es igual al grado de trascendencia de la extensión $K(X_1,\ldots,X_n)/K$, que es igual a n.
Para cada K–álgebra íntegra A llamamos $\tau(A)$ el máximo de los s tales que existe un subconjunto $\{a_1,\ldots,a_s\}\subseteq A$ algebraicamente independiente.
Hacemos la demostración del teorema en dos partes:
(1). Si $0\neq\mathfrak{p}\subseteq A$ es un ideal primo, entonces $\tau(A/\mathfrak{p})\geq s$ implica $\tau(A)\geq s+1$.
Supongamos que $\tau(A/\mathfrak{p})=s$, y sean $\{a_1,\ldots,a_s\}\in A$ tales que $\{\overline{a_i}=a_i+\mathfrak{p}\}_{i=1}^s$ es algebraicamente independiente. Tomamos $0\neq a\in\mathfrak{p}$, entonces $\{a_1,\ldots,a_s,a\}$ es algebraicamente independiente. En efecto, si existe $0\neq F\in K[Y_1,\ldots,Y_{s+1}]$ tal que $F(a_1,\ldots,a_s,a)=0$, tomando clases módulo $\mathfrak{p}$ se tiene $F(\overline{a_1},\ldots,\overline{a_s},0)=0$, y como $\{\overline{a_i}\}_{i=1}^s$ es algebraicamente independiente, resulta que $F(Y_1,\ldots,Y_s,0)=0$, esto es, $Y_{s+1}\mid F$. Si inicialmente tomamos F irreducible, resulta que $F=Y_{s+1}$, esto es, $a=0$, lo que es una contradicción.
(2). Si $0=\mathfrak{p}_0\subsetneqq\mathfrak{p}_1\subsetneqq\cdots\subsetneqq\mathfrak{p}_t$ es una cadena de ideales primos en $K[X_1,\ldots,X_n]$, entonces tenemos:

$$n\geq\tau\left(\frac{K[X_1,\ldots,X_n]}{\mathfrak{p}_0}\right)>\tau\left(\frac{K[X_1,\ldots,X_n]}{\mathfrak{p}_1}\right)>\cdots>\tau\left(\frac{K[X_1,\ldots,X_n]}{\mathfrak{p}_t}\right)\geq 0.$$

Y por lo tanto se tiene $n\geq t$. □

Lema de normalización

Como se observa, el estudio de los subconjuntos algebraicamente independientes de álgebras finitamente generadas aporta información sobre la misma álgebra. Vamos a ver que podemos obtener más información al considerar las subalgebras maximales generadas por estos subconjuntos.

Veamos un primer resultado técnico.

Lema. 36.5. (Lema de normalización.)
Sea $A = K[X_1,\ldots,X_n]$ un anillo de polinomios y sea $\mathfrak{p} \subsetneq A$ un ideal primo de altura s. Existen elementos $x_1,\ldots,x_n \in A$, algebraicamente independientes sobre K, tales que:

(1) A es entero sobre $B = K[x_1,\ldots,x_n]$ y
(2) si $\mathfrak{p} \neq 0$, $\mathfrak{p} \cap B$ está generado por $x_1,\ldots,x_s$.

DEMOSTRACIÓN. Hacemos inducción sobre la altura s de $\mathfrak{p}$. Si $\operatorname{ht}(\mathfrak{p}) = 0$, entonces $\mathfrak{p} = 0$ y podemos tomar $x_i = X_i$, $1 \leq i \leq n$, y tenemos el resultado.

Supongamos pues que $\operatorname{ht}(\mathfrak{p}) = 1$. Sea $0 \neq F \in \mathfrak{p}$, irreducible. Llamamos $x_1 = F(X_1,\ldots,X_n) = \sum_{\alpha\in\mathbb{N}^n} k_\alpha X^\alpha$. Tomamos $p_1 = 1$ y sean $p_2,\ldots,p_n$, enteros primos distintos; para cada $\alpha \in \mathbb{N}^n$ definimos $w(\alpha) = \sum_{i=1}^n p_i\alpha_i$. Es claro que, fijado F, podemos elegir los p_i de forma que dados dos exponentes $\alpha \neq \beta$, entonces $w(\alpha) \neq w(\beta)$. De esta forma, si definimos $x_i = X_i - X_1^{p_i}$ para $i = 2,\ldots,n$, se tiene:

$$x_1 = F(X_1,\ldots,X_n) = F(X_1, x_2 + X_1^{p_2},\ldots,x_n - X_1^{p_n}) = G(X_1,x_2,\ldots,x_n) + aX_1^e.$$

Siendo e el mayor grado con el que aparece ahora X_1 en F y G un polinomio en el que el grado de X_1 es menor que e. Es claro que $a \neq 0$, y por tanto es invertible.

Se tiene que X_1 es entero sobre $K[x_1,\ldots,x_n]$, ya que es raíz de un polinomio mónico. En consecuencia cada X_i es entero sobre $K[x_1,\ldots,x_n]$ y la extensión $B = K[x_1,\ldots,x_n] \subseteq K[X_1,\ldots,X_n]$ es entera.

Tenemos $x_1 \in \mathfrak{p}\cap B$, y por tanto $Bx_1 \subseteq \mathfrak{p}\cap B$; ambos son ideales primos, y por el Teorema del descenso la altura de $\mathfrak{p}\cap B$ es uno, entonces son iguales.

Como $K[X_1,\ldots,X_n]$ es entero sobre $K[x_1,\ldots,x_n]$, tenemos que $K(X_1,\ldots,X_n)$ es algebraico sobre el cuerpo $K(x_1,\ldots,x_n)$. Como el grado de trascendencia de $K(X_1,\ldots,X_n)$ sobre K es igual a n, lo mismo ocurre para $K(x_1,\ldots,x_n)$, luego los x_1, …, x_n son algebraicamente independientes sobre K, y $B = K[x_1,\ldots,x_n]$ es un anillo de polinomios.

Sea ahora $\mathfrak{p}$ un ideal primo de altura $h > 1$; tomamos $\mathfrak{q} \subseteq \mathfrak{p}$ un ideal primo de altura $h-1$. Por la hipótesis de inducción existen $x_1,\ldots,x_n \in A$ tales que $\mathfrak{q}\cap B = B(x_1,\ldots,x_{h-1})$. Consideramos el anillo $B/(\mathfrak{q}\cap B) \cong K[x_h,\ldots,x_n]$ y el ideal $(\mathfrak{p}\cap B)/(\mathfrak{q}\cap B)$. Éste tiene altura uno, por lo tanto existen $y_h,\ldots,y_n \in K[x_h,\ldots,x_n]$ tales que la extensión $K[y_h,\ldots,y_n] \subseteq K[x_h,\ldots,x_n]$ es entera y tenemos $\frac{\mathfrak{p}\cap B}{\mathfrak{q}\cap B} \cap K[y_h,\ldots,y_n] = K[y_h,\ldots,y_n]y_h$.

En consecuencia la extensión $C = K[x_1,\ldots,x_{h-1},y_h,\ldots,y_n] \subseteq K[X_1,\ldots,X_n]$ es entera y se tiene $\mathfrak{p}\cap C = C(x_1,\ldots,x_{h-1},y_h)$. □

Corolario. 36.6.
Sea K un cuerpo, entonces el ideal $(X_1,\ldots,X_s)$ tiene altura s en $K[X_1,\ldots,X_n]$, siendo $s \leq n$.

Teorema de normalización

Sea trata ahora de determinar la dimensión de una K–álgebra íntegra y finitamente generada A siguiendo el método empleado para el caso del anillo de polinomios.

Teorema. 36.7. (Teorema de normalización.)
Sea A una K–álgebra íntegra finitamente generada. Existen elementos $a_1,\ldots,a_t \in A$, algebraicamente independientes, tales que $K[a_1,\ldots,a_t] \subseteq A$ es entera.

DEMOSTRACIÓN. Existe un anillo de polinomios $K[X_1,\ldots,X_n]$ y un ideal primo $\mathfrak{p}$ tales que $A \cong K[X_1,\ldots,X_n]/\mathfrak{p}$. Por el lema de normalización existen $x_1,\ldots,x_n \in K[X_1,\ldots,X_n]$ y $s \in \mathbb{N}$ tales que $K[x_1,\ldots,x_n] \subseteq K[X_1,\ldots,X_n]$ es entera y $\mathfrak{p} \cap K[x_1,\ldots,x_n] = K[x_1,\ldots,x_n](x_1,\ldots,x_s)$. Entonces la extensión

$$K[x_{s+1},\ldots,x_n] \cong \frac{K[x_1,\ldots,x_n]}{\mathfrak{p} \cap K[x_1,\ldots,x_n]} \subseteq \frac{K[X_1,\ldots,X_n]}{\mathfrak{p}} \cong A$$

es una extensión entera y $\{x_{s+1}+\mathfrak{p},\ldots,x_n+\mathfrak{p}\} \subseteq A$ es un conjunto algebraicamente independiente. □

Corolario. 36.8.
Sea A una K–álgebra íntegra finitamente generada, entonces la dimensión de A es igual al grado de trascendencia del cuerpo de fracciones de A.

DEMOSTRACIÓN. Aplicamos el Teorema de normalización. Existe una subálgebra B de A, isomorfa a $K[X_1,\ldots,X_n]$, tal que A es entero sobre B. Como consecuencia $\dim(A) = \dim(B) = s$. Por otro lado, si llamamos L al cuerpo de fracciones de A, tenemos una extensión algebraica $K(X_1,\ldots,X_n) \subseteq L$, y el grado de trascendencia de L es igual a n. □

Corolario. 36.9.
Sea A una K–álgebra finitamente generada y $\mathfrak{p}$ un ideal primo de A. Se verifica que la dimensión del álgebra $A/\mathfrak{p}$ es exactamente el grado de trascendencia del cuerpo de fracciones de $A/\mathfrak{p}$.

Corolario. 36.10.
Sea A una K–álgebra íntegra finitamente generada y $\mathfrak{p} \subseteq A$ un ideal primo. Se verifica:

$$\dim(A) = \dim(A/\mathfrak{p}) + ht(\mathfrak{p}).$$

DEMOSTRACIÓN. Podemos reducir el problema a considerar A un anillo de polinomios. En este contexto el resultado es una consecuencia directa del Teorema de normalización de Noether. □

Demostración directa.

DEMOSTRACIÓN. Por el Lema de normalización existe una subálgebra $B \cong K[x_1,\dots,x_n]$ de A tal que A es entero sobre B y $\mathfrak{p}\cap B = B(x_1,\dots,x_s)$ para algún $s \leq n$. Tenemos $\operatorname{ht}(\mathfrak{p}\cap B) = s$ y por otro lado $B/(\mathfrak{p}\cap B) \cong K[X_{s+1},\dots,X_n]$, luego $\dim(B/(\mathfrak{p}\cap B)) = n-s$.
Como A es entero sobre B tenemos que $\dim(A) = \dim(B) = n$. Además $A/\mathfrak{p}$ es entero sobre $B/(\mathfrak{p}\cap B)$, luego $\dim(A/\mathfrak{p}) = \dim(B/(\mathfrak{p}\cap B)) = n-s$.
Como B es un dominio normal, el teorema del descenso nos asegura que si $\operatorname{ht}(\mathfrak{p}\cap B) = s$, entonces $\operatorname{ht}(\mathfrak{p}) = s$. Uniendo todo tenemos el resultado. □

Una cadena de ideales primos $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ se llama **maximal** si $\mathfrak{p}_0$ es minimal, $\mathfrak{p}_n$ es maximal y no existe ningún ideal primo $\mathfrak{q}$ tal que $\mathfrak{p}_{i-1} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}_i$, para $1 \leq i \leq n$.

Teorema. 36.11.
Sea A una K–álgebra íntegra finitamente generada, entonces todas las cadenas maximales de ideales primos de A tienen la misma longitud.

DEMOSTRACIÓN. Sea $\mathfrak{p}_0 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n$ una cadena maximal de ideales primos de A. Entonces $\mathfrak{p}_n$ es un ideal maximal y $\dim(A/\mathfrak{p}_n) = 0$. Para $i \geq 1$ tenemos $\mathfrak{p}_{i-1} \subsetneqq \mathfrak{p}_i$ y $\mathfrak{p}_i/\mathfrak{p}_{i-1}$ es un ideal primo de $A/\mathfrak{p}_{i-1}$ de altura uno. Luego $\dim(A/\mathfrak{p}_i) + \operatorname{ht}(\mathfrak{p}_i/\mathfrak{p}_{i-1}) = \dim(A/\mathfrak{p}_{i-1})$, ó lo que es igual, $\dim(A/\mathfrak{p}_i) - \dim(A/\mathfrak{p}_{i-1}) = 1$. Tenemos entonces

$$\begin{aligned}\dim(A) &= \dim(A/\mathfrak{p}_0) - \dim(A/\mathfrak{p}_n)\\ &= \dim(A/\mathfrak{p}_0) - \dim(A/\mathfrak{p}_1) + \dim(A/\mathfrak{p}_1) - \dim(A/\mathfrak{p}_n)\\ &= (\dim(A/\mathfrak{p}_0) - \dim(A/\mathfrak{p}_1)) + \cdots + (\dim(A/\mathfrak{p}_{n-1}) - \dim(A/\mathfrak{p}_n)) = n.\end{aligned}$$

□

Ejemplo. 36.12.
Se considera el anillo $A = \mathbb{R}[X,Y]/(X^2-Y^3)$. Sabemos que A es un dominio que no es normal. Vamos a calcular un subanillo de polinomios maximal en A.
Tomamos $\mathfrak{p} = (X^2-Y^3) \subseteq \mathbb{R}[X,Y]$ y definimos:

$$\begin{aligned}x_1 &= X^2 - Y^3,\\ x_2 &= Y - X^2,\end{aligned}$$

Entonces $B = \mathbb{R}[x_1,x_2] \subseteq \mathbb{R}[X,Y]$ es una extensión entera y $\mathfrak{p}\cap B = Bx_1$.
Tenemos entonces que $\mathbb{R}[\overline{x_2}] \subseteq A$ es una extensión entera, siendo $\overline{x_2} = x_2 + \mathfrak{p}$. Si llamamos $x = X + \mathfrak{p}$, $y = Y + \mathfrak{p}$, entonces $\mathbb{R}[y - x^2] \subseteq A$ es una extensión entera.

37. Teorema de los ceros de Hilbert

Dado un cuerpo K, para cada ideal $\mathfrak{a}$ de $K[X_1,\dots,X_n]$ el conjunto de los ceros de $\mathfrak{a}$ es:

$$\mathcal{V}(\mathfrak{a}) = \{x \in \mathbb{A}^n(K) \mid P(x) = 0, \forall P \in \mathfrak{a}\}.$$

Es claro que si $\mathfrak{a} = K[X_1,\dots,X_n]$, entonces $\mathbb{V}(\mathfrak{a}) = \varnothing$, pero también puede ser que $\mathbb{V}(\mathfrak{a}) = \varnothing$ siendo $\mathfrak{a} \neq K[X_1,\dots,X_n]$. Por ejemplo, en $\mathbb{R}[X]$ el ideal $\mathfrak{a} = (X^2+1)$ verifica $\mathcal{V}(X^2+1) = \varnothing$. Sin embargo si K es un cuerpo algebraicamente cerrado tenemos que $\mathcal{V}(\mathfrak{a}) \neq \varnothing$ si, y sólo si, $\mathfrak{a} \neq K[X]$.

Esta situación se repite en el caso de polinomios en varias indeterminadas.

Comenzamos por un resultado técnico.

Teorema. 37.1.
Si L/K es una extensión de cuerpos tal que L es una K–álgebra finitamente generada, entonces L es un K–módulo finitamente generado.

DEMOSTRACIÓN. Por el Teorema de Normalización se tiene que L es entero sobre $K[a_1,\dots,a_t]$ para cierto $\{a_1,\dots,a_t\} \subseteq L$ algebraicamente independiente. Aplicando la Proposición (35.12.) tenemos que $K[a_1,\dots,a_t]$ es un cuerpo, y por lo tanto se tiene $\{a_1,\dots,a_t\} = \varnothing$ y L es entero (algebraico) sobre K. Como es una K–álgebra finitamente generada, resulta que $\dim_K(L)$ es finita. □

Corolario. 37.2. (Teorema de los ceros de Hilbert. Forma débil.)
Sea K un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal de $K[X_1,\dots,X_n]$. Si $\mathcal{V}(\mathfrak{a}) = \varnothing$, entonces $\mathfrak{a} = K[X_1,\dots,X_n]$.

DEMOSTRACIÓN. Si $\mathfrak{a} \neq K[X_1,\dots,X_n]$, entonces existe un ideal maximal $\mathfrak{m} \supseteq \mathfrak{a}$, y como $\mathcal{V}(\mathfrak{m}) \subseteq \mathcal{V}(\mathfrak{a})$, basta considerar el caso en que $\mathfrak{a}$ es un ideal maximal. En este caso tendremos un homomorfismo (no nulo) $K \longrightarrow \frac{K[X_1,\dots,X_n]}{\mathfrak{a}} =: L$, y K es un subcuerpo de un cuerpo L.

Consideramos la extensión L/K; por el Teorema anterior se tiene esta extensión es finita, y por ser K algebraicamente cerrado $L = K$.

Como $L = K$, para cada índice $i = 1,\dots,n$ existe un elemento $a_i \in K$ que es la imagen de X_i. Por tanto $X_i - a_i \in \mathfrak{a}$, obteniendo que $(X_1 - a_1,\dots,X_n - a_n) \subseteq \mathfrak{a}$, y por tanto $(X_1 - a_1,\dots,X_n - a_n) = \mathfrak{a}$, obteniendo que $(a_1,\dots,a_n) \in \mathcal{V}(\mathfrak{a}) \neq \varnothing$. □

El resultado central de esta sección es:

Teorema. 37.3. (Teorema de los ceros de Hilbert.)
Sea K un cuerpo algebraicamente cerrado y $\mathfrak{a}$ un ideal de $K[X_1,\dots,X_n]$. Entonces $\operatorname{rad}(\mathfrak{a}) = \mathcal{IV}(\mathfrak{a})$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{a} = (F_1,\dots,F_t)$. Si $F \in \mathcal{IV}(\mathfrak{a})$ entonces consideramos $\widetilde{\mathfrak{a}} = (F_1,\dots,F_n, 1-YF) \subseteq K[X_1,\dots,X_n,Y]$. Vamos a ver que $\mathcal{V}(\widetilde{\mathfrak{a}}) = \varnothing$.
Sea $(a_1,\dots,a_n,a_{n+1}) \in \mathcal{V}(\widetilde{\mathfrak{a}}) \subseteq \mathbb{A}^{n+1}(K)$, entonces $(a_1,\dots,a_n) \in \mathcal{V}(\mathfrak{a})$, y resulta $F(a_1,\dots,a_n) = 0$, por lo tanto $0 = 1-a_{n+1}F(a_1,\dots,a_n) = 1$, lo que es una contradicción. Como consecuencia $\mathcal{V}(\widetilde{\mathfrak{a}}) = \varnothing$.
Aplicando el Teorema de Hilbert en su forma débil resulta $\widetilde{\mathfrak{a}} = K[X_1,\dots,X_n,Y]$, por lo que existe una combinación lineal

$$1 = \sum_i F_iC_i + (1-YF)C, \qquad C_1,\dots,C_t,C \in K[X_1,\dots,X_n,Y].$$

Tomando $Y = 1/F(X_1,\dots,X_n)$ tenemos:

$$1 = \sum_i F_i(X_1,\dots,X_n)C_i(X_1,\dots,X_n,\frac{1}{F(X_1,\dots,X_n)}),$$

y multiplicando por una potencia adecuada de F se tiene:

$$F^m = \sum_i F_i(X_1,\dots,X_n)D_i(X_1,\dots,X_n) \in \mathfrak{a}.$$

Como consecuencia $\mathcal{IV}(\mathfrak{a}) \subseteq \operatorname{rad}(\mathfrak{a})$. Por otro lado la inclusión inversa es siempre cierta ya que $\mathcal{IV}(\mathfrak{a})$ es un ideal radical que contiene a $\mathfrak{a}$.
La inclusión $\operatorname{rad}(\mathfrak{a}) \subseteq \mathcal{IV}(\mathfrak{a})$ya la conocemos. □

Consecuencias del Teorema de los Ceros

Por el Teorema de los ceros de Hilbert, sobre un cuerpo algebraicamente cerrado K existe una correspondencia biyectiva, que invierte el orden, entre los conjuntos algebraicos de $\mathbb{A}^n(K)$ y los ideales radicales del anillo $K[X_1,\dots,X_n]$.
Otras consecuencias del Teorema de los ceros son:
Un conjunto algebraico $V \subseteq \mathbb{A}^n(K)$ se llama **irreducible** si cuando $V = V_1 \cup V_2$, para conjuntos algebraicos V_i se tiene $V = V_1$ o $V = V_2$.

Lema. 37.4.
Si V es un conjunto algebraico afín irreducible, si y solo si, $\mathcal{I}(V)$ es un ideal primo.

DEMOSTRACIÓN. Si $V = \mathcal{V}(\mathfrak{c})$ es irreducible y $\mathfrak{ab} \subseteq \mathcal{I}(V) = \mathcal{I}\mathcal{V}(\mathfrak{c})$, entonces $V = \mathcal{V}\mathcal{I}\mathcal{V}(\mathfrak{c}) \subseteq \mathcal{V}(\mathfrak{ab}) = \mathcal{V}(\mathfrak{a}) \cup \mathcal{V}(\mathfrak{b}$. Entonces $V \subseteq \mathcal{V}(\mathfrak{a})$ o $V \subseteq \mathcal{V}(\mathfrak{b})$, y se tiene $\mathfrak{a} \subseteq \mathcal{I}\mathcal{V}(\mathfrak{a}) \subseteq \mathcal{I}(V)$ o $\mathfrak{b} \subseteq \mathcal{I}\mathcal{V}(\mathfrak{b}) \subseteq \mathcal{I}(V)$.

Recíprocamente, si $\mathcal{I}(V)$ es un ideal primo y $V = V_1 \cup V_2$, entonces $\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$. Luego $\mathcal{I}(V_1) = \mathcal{I}(V)$ o $\mathcal{I}(V_2) = \mathcal{I}(V)$, de donde se obtiene $V_1 = V$ o $V_2 = V$. □

Corolario. 37.5.
Sea K un cuerpo algebraicamente cerrado. Si $\mathfrak{p}$ es un ideal primo de $K[X_1, \ldots, X_n]$, entonces $V(\mathfrak{p})$ es un conjunto algebraico irreducible. Existe entonces una correspondencia biyectiva entre ideales primos y conjuntos algebraicos irreducibles. En esta correspondencia a los ideales maximales le corresponden los puntos.

Corolario. 37.6.
Sea K un cuerpo algebraicamente cerrado. Sea $F \in K[X_1, \ldots, X_n]$ un polinomio con factorización $F = F_1^{e_1} \cdots F_r^{e_r}$ en factores irreducibles, entonces

$$\mathcal{V}(F) = \mathcal{V}(F_1) \cup \cdots \cup \mathcal{V}(F_r)$$

es la descomposición de $\mathcal{V}(F)$ en componentes irreducibles. Además, $\mathcal{I}\,\mathcal{V}(F) = (F_1 \cdots F_r)$. En particular, existe una correspondencia biyectiva entre polinomios irreducibles $F \in K[X_1, \ldots, X_n]$ e hipersuperficies irreducibles de $\mathbb{A}^n$.

Corolario. 37.7.
Sea $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$, tenemos que son equivalentes:
(a) $\mathcal{V}(\mathfrak{a})$ es un conjunto finito;
(b) $K[X_1, \ldots, X_n]/\mathfrak{a}$ es un K–espacio vectorial de dimensión finita.

En este caso el número de puntos de $\mathcal{V}(\mathfrak{a})$ está acotado por la dimensión $\dim_K(K[X_1, \ldots, X_n]/\mathfrak{a})$.

DEMOSTRACIÓN. Sean $x^1, \ldots, x^r \in V(\mathfrak{a})$, tomamos

$$F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$$

tales que $F_i(x^j) = \delta_{ij}$, y llamamos $F_i + \mathfrak{a}$ a la clase de F_i en $K[X_1, \ldots, X_n]/\mathfrak{a}$. Si existe una combinación

$$\sum a_i(F_i + \mathfrak{a}) = 0,$$

entonces $\sum a_iF_i \in \mathfrak{a}$. Para cada índice i tenemos

$$0 = (\sum a_iF_i)(x^i) = a_iF_i(x^i) = a_i.$$

Y por tanto $\{F_1 + \mathfrak{a}, \ldots, F_r + \mathfrak{a}\}$ son linealmente independientes, luego $r \leq \dim_K(K[X_1, \ldots, X_r]/\mathfrak{a})$. Recíprocamente, si $\mathcal{V}(\mathfrak{a}) = \{x^1, \ldots, x^r\}$ es finito, supongamos que $x^i = (x^i_1, \ldots, x^i_n)$, y definimos

$$F_j = \prod_{i=1}^{r}(X_j - x^i_j).$$

De la definición se deduce que $F_j \in \mathcal{I}\,\mathcal{V}(\mathfrak{a})$, entonces existe $m \in \mathbb{N}$ tal que $F_j^m \in \mathfrak{a}$. Considerando ahora las clases $F_j^m + \mathfrak{a} = 0$, se deduce que $X_j^{mr} + \mathfrak{a}$ es una combinación K–lineal de potencias de $X_j + \mathfrak{a}$ con exponente menor que mr. En consecuencia, tenemos un sistema de generadores $\{X_1^{e_1} \cdots X_n^{e_n} + \mathfrak{a} \mid e_i < mr\}$ y $K[X_1, \ldots, X_n]/\mathfrak{a}$ es un K–espacio vectorial de dimensión finita. □

38. Extensiones trascendentes (repaso)

Sean K y F cuerpos tales que $K \subseteq F$ es un subcuerpo; entonces decimos que F es una **extensión de cuerpos** de K. Es claro que F es un K–espacio vectorial. Si $\dim_K(F) < \infty$, la extensión se llama de **dimensión finita**, e **infinita** en caso contrario.

Dada una extensión F/K, y un elemento $\alpha \in F$, definimos una homomorfismo de anillos $f_\alpha : K[X] \to F$ mediante $f_\alpha(X) = \alpha$. El núcleo de f_α es un ideal primo generado por un polinomio, sea F_α. Si $F_\alpha \neq 0$, entonces $F_\alpha(\alpha) = 0$, y decimos que α es **algebraico** sobre K; en este caso $\mathrm{Im}(F_\alpha) = K[\alpha]$ es un cuerpo y la extensión $K[A]/K$ es de dimensión finita, y si $F_\alpha = 0$, entonces decimos que α es **trascendente** sobre K; en este caso $\mathrm{Im}(F_\alpha = K[\alpha]$ es isomorfo a un anillo de polinomios; su anillo de fracciones se representa por $K(\alpha)$ y la extensión de $K(\alpha)/K$ es de dimensión infinita. Por extensión, aún en el caso de α algebraico sobre K, la extensión $K[\alpha]/K$ se representa también por $K(\alpha)/K$.

Una extensión F/K es **algebraica** si todo elemento de F es algebraico sobre K, y es **trascendente pura** si ningún elemento de $F \setminus K$ es algebraico sobre K.

Lema. 38.1.
Dada una torre de cuerpos $K \subseteq F \subseteq L$, se verifica: L/K es una extensión algebraica si, y sólo si, L/F y F/K son extensiones algebraicas.

Lema. 38.2.
Dada una extensión F/K el conjunto $E_K^F = \{\alpha \in F \mid \alpha \text{ es algebraico sobre } K\}$ es un cuerpo tal que $K \subseteq E_K^F \subseteq F$. La extensión E_K^F/K es algebraica, y la extensión F/E_K^F es trascendente pura.

El cuerpo E_K^F se llama la **clausura algebraica** de K en F.

Lema. 38.3.
*Dadas torres de cuerpos $K \subseteq F_1, F_2 \subseteq L$, existe un menor subcuerpo F de L tal que $K \subseteq F_1, F_2 \subseteq F \subseteq L$. Llamamos a este cuerpo F la **composición** de F_1 y F_2, y lo representamos por F_1F_2.*

Dada una extensión F/K y extensiones $K \subseteq K(\alpha), K(\beta) \subseteq F$, la composición se representa simplemente por $K(\alpha, \beta)$; y ser llama una **extensión finitamente generada**. Por extensión podemos considerar extensiones finitamente generadas del tipo $K(\alpha_1, \ldots, \alpha_t)/K$.

Observación. 38.4.
A veces utilizamos el término extensión finita indiferentemente para extensiones F/K de dimensión finita y para extensiones finitamente generadas. Su significado se deduce en cada caso del contexto.

Sea $K \subseteq L$ una extensión finita de cuerpos.

Un conjunto finito $\{x_1, \ldots, x_n\} \subseteq L$ de elementos de L se llama **algebraicamente independiente** sobre K si no existe un polinomio $0 \neq F \in K[X_1, \ldots, X_n]$ tal que $F(x_1, \ldots, x_n) = 0$.

Una familia $\{x_i \mid i \in A\}$ se llama **algebraicamente independiente** si lo es cada subfamilia finita.

Un elemento $x \in L$ se llama **trascendente** sobre K si $\{x\}$ es una familia algebraicamente independiente.

Lema. 38.5.
Sea $K \subseteq L$ una extensión de cuerpos y $x_1, \ldots, x_n \in L$ elementos distintos. Son equivalentes:

(a) $\{x_1, \ldots, x_n\}$ es algebraicamente independiente sobre K;
(b) Para cada $1 < s < n$ la familia $\{x_1, \ldots, x_s\}$ es algebraicamente independiente sobre K y $\{x_{s+1}, \ldots, x_n\}$ es algebraicamente independiente sobre $K(x_1, \ldots, x_s)$.

Sea $K \subseteq L$ una extensión de cuerpos. Una familia $\{x_1, \ldots, x_n\} \subseteq L$ se llama una **base de trascendencia** de L sobre K si verifica:

(I) $\{x_1, \ldots, x_n\}$ es algebraicamente independiente sobre K;

(II) L es algebraico sobre $K(x_1, \ldots, x_n)$.

Lema. 38.6.
Dada una extensión de cuerpos $K \subseteq L$, un conjunto $X \subseteq L$ es una base de trascendencia si es un conjunto algebraicamente independiente maximal.

Lema. 38.7.
Sea $K \subseteq L$ una extensión de cuerpos y $x_1, \ldots, x_n \in L$ tales que $K(x_1, \ldots, x_n) \subseteq L$ es algebraica. Se verifica:

(1) Todo subconjunto de $\{x_1, \ldots, x_n\}$ algebraicamente independiente sobre K, maximal para la inclusión, es una base de trascendencia de L sobre K;
(2) Si $\{x_1, \ldots, x_s\}$, $s \leq n$ es algebraicamente independiente sobre K, entonces existe una base de trascendencia de L sobre K que contiene a $\{x_1, \ldots, x_s\}$ y contenida en $\{x_1, \ldots, x_n\}$.

Como consecuencia las bases de trascendencia son subconjuntos algebraicamente independientes maximales respecto a la inclusión, y cada extensión de cuerpos $K \subseteq L$ tiene una base de trascendencia.

Teorema. 38.8.
Dada una extensión de cuerpos $K \subseteq L$ se verifica:

(1) Todo subconjunto $X \subseteq L$ tal que al extensión $L/K(X)$ es algebraica contiene una base de trascendencia de la extensión $L(K)$.
(2) Dado un conjunto algebraicamente independiente $\{x_1,\ldots,x_n\}$ y un conjunto $\{a_1,\ldots,a_m\} \subseteq L$ tal que la extensión $L/K(a_1,\ldots,a_m)$ es algebraica, existe una ordenación de $\{a_1,\ldots,a_m\}$ tal que para cada índice $i=1,\ldots,n$ la extensión $L/K(x_1,\ldots,x_i,a_{i+1},\ldots,a_m)$ es algebraica.
(3) El número de elementos de una base de trascendencia es un invariante.

Este invariante se llama **grado de trascendencia** de la extensión y lo vamos a representar por $\operatorname{grtr}(L/K)$. Una extensión es algebraica si, y sólo si, su grado de trascendencia es igual a cero.

Corolario. 38.9.
Si K es un cuerpo, el grado de trascendencia del cuerpo $K(X_1,\ldots,X_n)$, el cuerpo de fracciones del anillo de polinomios $K[X_1,\ldots,X_n]$, es igual a n.

Teorema. 38.10.
Sea K un cuerpo. Dado un elemento trascendente X sobre K y polinomios $F,G \in K[X]$ no nulos, primos relativos y no siendo los dos constantes, entonces

(1) F/G es trascendente sobre K
(2) $[K(X):K(F/G)] = max\{gr(F),gr(G)\}$.
(3) Para cualquier cuerpo intermedio $K \subsetneqq L \subseteq K(X)$, la extensión $K(X)/L$ es algebraica.
(4) Toda K–álgebra $K \subsetneqq A \subseteq K[X]$ es de dimensión de Krull igual a uno.

DEMOSTRACIÓN. (1). Consideramos el polinomio $H(Y) = G(Y)\frac{F(X)}{G(X)} - F(Y) \in K(F/G)[Y]$, que se anula para $Y = X$, y por lo tanto X es algebraico sobre $K(F/G)$, y F/G es trascendente sobre K, pues $\operatorname{grtr}(K(X)/K) = 1$.
(2). El grado de H es el máximo de $\{gr(F),gr(G)\}$, y H es irreducible en $K(F/G)[Y]$, ya que si $H = H_1H_2$ es una factorización, existen polinomios primitivos $K_1,K_2 \in K[F/G][Y]$, y un polinomio $K_0 \in K[F/G]$ tales que $H = K_0(F/G)K_1(F/G,Y)K_2(F/G,Y)$. Pero como H tiene grado uno en F/G, entonces K_1 ó K_2 pertenece a $K[Y]$; supongamos que es K_2. Se tiene $K_0(F/G)K_1(F/G,Y)K_2(F/G,Y) = G(Y)\frac{F(X)}{G(X)} - F(Y)$; si hacemos $F/G = 0$, tenemos $K_2 \mid F$; si hacemos $F/G = 1$, tenemos $K_2 \mid G$, y por tanto K_2 es constante, y H es irreducible.
(3). Es claro, estudiando, por ejemplo, los grados de trascendencia.

(4). Es claro que $\mathrm{Kdim}(A) \geq 1$; si en A tenemos dos elementos algebraicamente independientes sobre K, como éstos pertenecen a $K[X]$, resulta que $\mathrm{Kdim}(K[X]) \geq 2$, lo que es imposible. □

Teorema. 38.11. (Teorema de Lüroth.)
Dado un elemento trascendente x sobre K, para todo cuerpo intermedio L tal que $K \subseteq L \subseteq K(x)$ existe $y \in K(x)$ tal que $L = K(y)$. En particular toda extensión intermedia $K \subseteq L \subseteq K(x)$ es una extensión trascendente pura.

DEMOSTRACIÓN. Dado $z = F(x)/G(x) \in L \setminus K$, con $F, G \in K[X]$ coprimos, tenemos

$$m = [K(x) : L] \leq [K(x) : K(F/G)] = \max\{gr(F), gr(G)\} =: d_z.$$

Se trata de encontrar z tal que $m = d_z$.
Sea $F = \mathrm{Irr}(x, L) = Y^m + \frac{a_{m-1}}{b_{m-1}} Y^{m-1} + \cdots + \frac{a_1}{b_1} Y + \frac{a_0}{b_0}$, con $\frac{a_i}{b_i} \in L \subseteq K(x)$, $a_i(X), b_i(X) \in K[X]$ coprimos. Como x no es algebraico sobre K, algún $\frac{a_i}{b_i} \notin K$. Definimos $z = \frac{a_i}{b_i}$ y $d = d_z$; se tiene $m \leq d$.
Definimos $G = a_i(Y) - \frac{a_i(x)}{b_i(x)} b_i(Y) \in L[Y]$, que verifica $G(x) = 0$, luego $\mathrm{Irr}(x, L) \mid G$, y existe $H \in L[Y]$ tal que $G = H \,\mathrm{Irr}(x, L) = HF$; esto es, $a_i(Y)b_i(x) - a_i(x)b_i(Y) = b_i(x)HF$. Multiplicando por $b_0(x) \cdots b_{m-1}(x)$ se tiene

$$b_0(x) \cdots b_{m-1}(x)(a_i(Y)b_i(x) - a_i(x)b_i(Y)) = b_i(x)H(b_0(x) \cdots b_{m-1}(x))F.$$

Desarrollamos

$$G_1 := (b_0(x) \cdots b_{m-1}(x))F =$$
$$b_0(x) \cdots b_{m-1}(x)Y^m + \sum_{j=0}^{m-1} b_0(x) \cdots b_{k-1}(x)a_k(x)b_{k+1}(x) \cdots b_{m-1}(x)Y^{m-1} \in K[x][Y]$$

Si $G_0(x)$ es el contenido de G_1 en $K[x]$, tenemos una factorización $G_1[x, Y] = G_0(x)G_2(x, Y)$, y ningún polinomio no contante de $K[x]$ divide a $G_2(x, Y)$. Como $G_0(x)$ divide a $b_0(x) \cdots b_{m-1}(x)$ y también divide a $b_0(x) \cdots b_{i-1}(x)a_i(x)b_{i+1}(x) \cdots b_{m-1}(x)$, divide a su mcd, y por tanto divide también a $b_0(x) \cdots b_{i-1}(x)b_{i+1}(x) \cdots b_{m-1}(x)$. En consecuencia $b_i(x)$ divide al coeficiente de Y_m en G_2, y $a_i(x)$ divide al coeficiente de Y^i. Entonces $\mathrm{gr}_x(G_2(x, Y)) \geq \max\{\mathrm{gr}(a_i(x)), \mathrm{gr}(b_i(x))\} = d$.
Como $H \in L[Y]$, podemos escribir $H = \frac{H_1(x,Y)}{H_0(x)}$, y podemos escribir

$$H_0(x)b_0(x) \cdots b_{m-1}(x)(a_i(Y)b_i(x) - a_i(x)b_i(Y)) = b_i(x)H_1(x, Y)G_0(x)G_2(x, Y).$$

Por ser $G_2(x, Y)$ primitivo en $K[x]$, tenemos $H_0(x)b_0(x) \cdots b_{m-1}(x) \mid b_i(x)H_1(x, Y)G_0(x)$, y existe $H_2 \in K[x, Y]$ tal que $b_i(x)H_1(x, Y)G_0(x) = H_2(x, Y)H_0(x)b_0(x) \cdots b_{m-1}(x)$, y se tiene

$$a_i(Y)b_i(x) - a_i(x)b_i(Y) = H_2(x, Y)G_2(x, Y).$$

El grado en x de $a_i(Y)b_i(x) - a_i(x)b_i(Y)$ es menor o igual que d. El grado en x de $G_2(x,Y)$, como hemos visto, mayor o igual que d. Esto significa que el grado en x de $H_2(x,Y)$ es cero, y tenemos $H_2(x,Y) = H_2(Y) \in K[Y]$.

Escribimos en $a_i(Y)b_i(x) - a_i(x)b_i(Y) = H_2(Y)G_2(x,Y)$; el miembro de la izquierda es antisimétrico en x e Y, y el de la derecha no es divisible por ningún polinomio no constante en x, luego $H_2(Y)G_2(x,Y)$ no tiene factores no constantes en Y; en particular $H_2(Y) = H_2 \in K$. En la expresión $a_i(Y)b_i(x) - a_i(x)b_i(Y) = H_2G_2(x,Y)$ el miembro de la izquierda tiene grados iguales en x e Y, por lo tanto se tiene

$$\operatorname{gr}_Y(G_2(x,Y)) = \begin{cases} \operatorname{gr}_Y(G_0(x)G_2(x,Y)) = \operatorname{gr}_Y(G_1(x,Y)) = \operatorname{gr}_Y(\operatorname{Irr}(x,L)) = m. \\ \operatorname{gr}_x(G_2(x,Y)) = \operatorname{gr}_x(a_i(Y)b_i(x) - a_i(x)b_i(Y)) \geq d \geq m. \end{cases}$$

Como consecuencia $m = d$ y $L = K(z)$. □

Teorema. 38.12. (Teorema de Castelnuovo.)
Dado K algebraicamente cerrado, $K \subseteq K(x_1,x_2)$ una extensión trascendente pura de grado de trascendencia dos, para cada cuerpo intermedio $K \subseteq L \subseteq K(x_1,x_2)$ tal que $K(x_1,x_2)/L$ es separable finita, la extensión L/K es trascendente.

Teorema. 38.13.
Dada una torre de cuerpos $K \subseteq L \subseteq F$ se verifica:

$$\operatorname{grtr}(F/K) = \operatorname{grtr}(F/L) + \operatorname{grtr}(L/K).$$

39. Ejercicios

Extensiones enteras

Ejercicio. 39.1.
Sea $A \subseteq B$ una extensión de anillos y $u_1, \ldots, u_t \in B$ elementos enteros sobre A, demuestra que $A[u_1, \ldots, u_t]$ es un A–módulo finitamente generado.

SOLUCIÓN

Ejercicio. 39.2.
Sea $A \subseteq B$ una extensión entera de anillos y $\mathfrak{p} \subseteq A$ un ideal primo. Demuestra que todo elemento $x \in \mathfrak{p}^e = B\mathfrak{p}$ (el extendido de $\mathfrak{p}$) satisface una ecuación $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$ con $a_i \in \mathfrak{p}$, $i = 0, \ldots, n-1$.

SOLUCIÓN

Ejercicio. 39.3.
Sea $A \subseteq B$ una extensión entera de anillos.

(1) Si $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots \subseteq \mathfrak{p}_n$ es una cadena de ideales primos distintos de A, demuestra que existe una cadena $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ldots \subseteq \mathfrak{q}_n$ de ideales primos distintos de B tales que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, n$.
(2) Si $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subseteq \ldots \subseteq \mathfrak{q}_n$ es una cadena de ideales primos distintos de B y $\mathfrak{p}_i = \mathfrak{q}_i \cap A$, para $i = 1, \ldots, n$, demuestra que $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \ldots \subseteq \mathfrak{p}_n$ es una cadena de ideales primos distintos de A.

SOLUCIÓN

Ejercicio. 39.4.
Sea $A \subseteq B$ una extensión entera de anillos.

(1) Si $a \in A$ es invertible en B, demuestra que a es invertible en A.
(2) Si todo ideal primo no nulo de A es maximal, demuestra que todo ideal primo de B es maximal.
(3) Demuestra que $J(A) = J(B)^c$.

SOLUCIÓN

Ejercicio. 39.5.
Sea A un dominio con cuerpo de fracciones K, sea F/K una extensión algebraica de cuerpos y B la clausura entera de A en F. Prueba que F es el cuerpo de fracciones de B.

SOLUCIÓN

Ejercicio. 39.6.
Estudia los siguientes enunciados:

(1) Prueba que si $\mathfrak{a}$ es un ideal maximal de A, nunca $\mathfrak{a}[X]$ es un ideal maximal de $A[X]$.
(2) Encuentra un ideal maximal $\mathfrak{m} \subseteq A[X]$ tal que $\mathfrak{a}[X] \subseteq \mathfrak{m}$.

SOLUCIÓN

Ejercicio. 39.7.
Dado un dominio de integridad A con cuerpo de fracciones K, para extensiones algebraicas $K(\alpha)$ y $K(\beta)$, prueba que no necesariamente la clausura entera de A en $K(\alpha,\beta)$ es la composición de las clausuras enteras en $K(\alpha)$ y $K(\beta)$.

SOLUCIÓN

Ejercicio. 39.8.
Sea A un dominio de integridad con cuerpo de fracciones K. Son equivalentes:

(a) $A = K$.
(b) K es un A–módulo finitamente generado.

Ver también el Ejercicio (29.22.). SOLUCIÓN

Ejercicio. 39.9.
Sea B un anillo conmutativo y $G \subseteq \mathrm{Aut}(B)$ un subgrupo finito del grupo de los automorfismos de B. Prueba:

(1) El conjunto $A = \{b \in B \mid g(b) = b \text{ para cada } g \in G\}$ es un subanillo de B.
(2) La extensión $A \subseteq B$ es una extensión entera.

SOLUCIÓN

Ejercicio. 39.10.
Sea K un cuerpo y A una K–álgebra de K–dimensión finita. Prueba que:

(1) La extensión $K \subseteq A$ es entera.
(2) A es un cuerpo si, y sólo si, A es un dominio de integridad.
(3) Si A es un anillo local con ideal maximal $\mathfrak{m}$ y $\dim_K(A) = n$, entonces $\mathfrak{m}^n = 0$.
(4) Da un ejemplo de K–álgebra local A con $\dim_K(A) = n$ tal que $\mathfrak{m}^{n-1} = 0$, y otro en el que $\mathfrak{m}^{n-1} \neq 0$.

SOLUCIÓN

Extensiones de anillos

Ejercicio. 39.11.
Llamamos finita a una extensión de anillos $A \subseteq B$ en la que B es un A–módulo finitamente generado, y finitamente generada si B es una A–álgebra finitamente generada.

(1) Prueba que toda extensión finita es finitamente generada.
(2) Da un ejemplo de una extensión finitamente generada que no sea finita.
(3) Dadas extensiones finita $A \subseteq B$ y $B \subseteq C$, prueba que la extensión $A \subseteq C$ es finita.
(4) Dada una extensión de anillos $A \subseteq B$, son equivalentes:
  - *(a) La extensión $A \subseteq B$ es finita.*
  - *(b) La extensión $A \subseteq B$ finitamente generada y entera.*

SOLUCIÓN

Ejercicio. 39.12.
Sea A un anillo local, $A \subseteq B$ una extensión de anillos y B un A–módulo finitamente generado. Prueba que B es un anillo semilocal.

SOLUCIÓN

Ejercicio. 39.13.
Sea $A \subseteq B$ una extensión entera, $\mathfrak{p} \subseteq A$ un ideal primo y B un A–módulo finitamente generado. Prueba que existe sólo un número finito de ideales primos $\mathfrak{q} \subseteq B$ tales que $\mathfrak{p} = \mathfrak{q} \cap A$.

SOLUCIÓN

Ejercicio. 39.14.
De los siguientes dominios ¿cuál es normal y cuál no lo es?

(1) $\mathbb{Z}[i]$.
(2) $\mathbb{Z}[\sqrt{5}]$.
(3) $\mathbb{Z}[\sqrt{-5}]$.
(4) $\mathbb{Z}[\omega]$, donde ω es una raíz cúbica primitiva de la unidad.
(5) $\mathbb{Z}[\sqrt{-3}]$.
(6) $\mathbb{Z}[\sqrt{6}]$.
(7) $\mathbb{Z}[i, \sqrt{2}]$.

SOLUCIÓN

Lema de normalización

Ejercicio. 39.15.
Sea $K \subseteq A$ una extensión de anillos finitamente generada. Si A es un cuerpo, entonces la extensión es finita (esto es, A es finitamente generado como K–espacio vectorial, o equivalentemente la extensión de cuerpos A/K es una extensión (algebraica) finita).

SOLUCIÓN

Ejercicio. 39.16.
Sea $f : A \to B$ un homomorfismo de K–álgebras finitamente generadas. Prueba que para todo ideal maximal $\mathfrak{n} \subseteq B$ se tiene que $\mathfrak{n} \cap A \subseteq A$ es un ideal maximal.

SOLUCIÓN

Ejercicio. 39.17.
Sea K un cuerpo. Demuestra que el ideal $(X^3 - Y^2)$ de $K[X, Y]$ es un ideal radical.

Este ejercicio se puede generalizar en la siguiente forma:

Sea K un cuerpo infinito. Si i y j son enteros positivos primos relativos, demuestra que $(X^i - Y^j)$ es un ideal radical en $K[X, Y]$.

SOLUCIÓN

Ejercicio. 39.18.
Sea K un cuerpo.

(1) Demuestra que el ideal $(X^2 - Y^3) \subseteq K[X,Y]$ es un ideal primo.
(2) Llamamos $T = \overline{X}/\overline{Y}$ en el cuerpo de fracciones del dominio $A := K[X,Y]/(X^2 - Y^3)$. Demuestra que $F = K(T)$ es el cuerpo de fracciones de A, y que $K[T]$ es la clausura entera de A en F.

SOLUCIÓN

Ejercicio. 39.19.
Sea D un dominio de integridad e i,j enteros positivos primos relativos.

(1) Demuestra que $(X^i - Y^j)$ es un ideal primo de $D[X,Y]$.
(2) Cuando $D = K$ es un cuerpo determina la normalización de $A := K[X,Y]/(X^i - Y^j)$.

SOLUCIÓN

Ejercicio. 39.20.
Sea K un cuerpo. Demuestra que el ideal $(Y^2 - X^3 - X^2)$ de $K[X,Y]$ es primo.

SOLUCIÓN

Ejercicio. 39.21.
Sea K un cuerpo y $\mathfrak{a} = (Y^2 - X^3 - X^2) \subseteq K[X,Y]$ un ideal.

(1) Demuestra que $\mathfrak{a}$ es un ideal primo de $K[X,Y]$.
(2) Determina la normalización del dominio de integridad $A := K[X,Y]/(Y^2 - X^3 - X^2)$.

SOLUCIÓN

Ejercicio. 39.22.
Calcula un subanillo de polinomios maximal en $A = \mathbb{R}[X,Y]/(XY - 1)$. Aplícalo para determinar la dimensión del anillo $K[X,X^{-1}]$.

SOLUCIÓN

Ejercicio. 39.23.
Determinar los ideales primos del anillo $\mathbb{C}[X,Y]$.

SOLUCIÓN

Ejercicio. 39.24.
Proponer un ejercicio sobre normalización con un ideal primo generado por dos o tres elementos.

SOLUCIÓN

Teorema de los ceros de Hilbert

Ejercicio. 39.25.
Sea $\mathfrak{a} = (F_1,\ldots,F_t)$ un ideal del anillo de polinomios $K[X_1,\ldots,X_n]$. Vamos a dar un algoritmo para determinar cuando un polinomio $F \in K[X_1,\ldots,X_n]$ pertenece al radical de $\mathfrak{a}$. Este algoritmo se basa en el siguiente hecho: Son equivalenteslos siguientes enunciados:

(a) $F \in \operatorname{rad}(\mathfrak{a})$.
(b) $1 \in (F_1,\ldots,F_t,1-YF) \subseteq K[X_1,\ldots,X_n,Y]$.

Entonces el algoritmo consiste en determinar una base de Groebner del ideal $(F_1,\ldots,F_t,1-YF)$ y ver si se reduce a $\{1\}$.

SOLUCIÓN

Ejercicio. 39.26.
Sea K un cuerpo de característica distinta de 2 y 3 y

$$\mathfrak{a} = (X^3+Y^3+Z^3, X^2+Y^2+Z^2, (X+Y+Z)^3) \subseteq K[X,Y,Z]$$

un ideal. Demuestra que $X,Y,Z \in \operatorname{rad}(\mathfrak{a})$.

SOLUCIÓN

Ejercicio. 39.27.
Sea K un cuerpo y $\mathfrak{a} = (X^4+Y^4+Z^4, X+Y+Z) \subseteq K[X,Y,Z]$.

(1) Si $\operatorname{car}(K) \neq 2$, utiliza bases de Groebner para comprobar que $XY+XZ+YZ \in \operatorname{rad}(\mathfrak{a})$ y determina la mínima potencia de $XY+XZ+YZ$ contenida en $\mathfrak{a}$.

(2) *Sea* $\mathfrak{b} = (X^4+Y^4+Z^4, X+Y+Z, XY+XZ+YZ) \subseteq K[X,Y,Z]$. *Comprueba que la base de Groebner reducida de* $\mathfrak{b}$ *respecto al orden lexicográfico* $X > Y > Z$ *es* $\{X+Y+Z, Y^2+YZ+Z^2\}$. *Deduce que* $K[X,Y,Z]/\mathfrak{b} \cong K[Y,Z]/(Y^2+YZ+Z^2)$, *y que* $\mathfrak{b}$ *es un ideal radical si car*$(K) \neq 3$.
(3) *Si car*$(K) \neq 2,3$, *demuestra que* $\operatorname{rad}(\mathfrak{a}) = \mathfrak{b}$.
(4) *Si car*$(K) = 3$, *demuestra que* $\operatorname{rad}(\mathfrak{a}) = (X-Y, Y-Z)$.
(5) *Si car*$(K) = 2$, *demuestra que* $\mathfrak{a} = (X+Y+Z)$ *es un ideal primo, y por tanto radical.*

SOLUCIÓN

Ejercicio. 39.28.
Sea $\mathfrak{a} = (X^2Y+Z^3, X+Y^3-Z, 2Y^4Z-YZ^2-Z^3) \subseteq K[X,Y,Z]$. *Utiliza bases de Groebner para probar que* $X, Y, Z \in \operatorname{rad}(\mathfrak{a})$ *y concluye que* $\operatorname{rad}(\mathfrak{a}) = (X,Y,Z)$. *Demuestra que* X^9, Y^7, Z^9 *son las mínimas potencias de* X, Y *y* Z, *respectivamente, que pertenecen en* $\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 39.29.
Sean $V = \mathcal{V}(X^3-X^2Z-Y^2Z)$, $W = \mathcal{V}(X^2+Y^2-Z^2)$ *conjuntos algebraicos de* $\mathbb{C}^3$. *Demuestra que* $\mathcal{I}(V) = (X^3-X^2Z-Y^2Z)$ *y* $\mathcal{I}(W) = (X^2+Y^2-Z^2)$ *en* $\mathbb{C}[X,Y,Z]$.

SOLUCIÓN

Ejercicio. 39.30.
Sea $V = \mathcal{V}(X^3+Y^3+7Z^3) \subseteq \mathbb{C}^3$. *Demuestra que* $\mathcal{I}(V) = (X^3+Y^3+7Z^3) \subseteq \mathbb{C}[X,Y,Z]$.

SOLUCIÓN

Ejercicio. 39.31.
Sea $\mathfrak{p}$ *un ideal de* $K[X_1,\ldots,X_n]$ *primo y principal, entonces ht*$(\mathfrak{p}) = 1$, *o equivalentemente se tiene* $\dim(K[X_1,\ldots,X_n]/\mathfrak{p}) = n-1$.
Observa que como una hipersuperficie es el conjunto de ceros de un polinomio, entonces cuando éste es irreducible, la hipersuperficie es de dimensión $n-1$.

SOLUCIÓN

Ejercicios del capítulo

Ejercicio. 39.32.
Sea A un anillo (conmutativo) y $x \in A$ un elemento tal que Ax es un ideal idempotente.

(1) *Prueba que Ax es un anillo (no necesariamente un subanillo de A).*
(2) *Prueba que existe un elemento $y \in A$ tal que $x = x^2 y$ e $y = xy^2$.*
(3) *El elemento y verificando la condición anterior es único.*
(4) *Si $e \in Ax$ es el elemento uno de Ax, entonces e es un elemento idempotente y $Ax = Ae$.*
(5) *En este caso se tiene una descomposición $A = Ae \oplus A(1-e)$.*

SOLUCIÓN

Ejercicio. 39.33.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos tal que $\mathrm{Ker}(f)$ es un ideal primo de A y la extensión $\mathrm{Im}(f) \subseteq B$ es entera.Prueba la verdad o falsedad, según el caso, de las siguientes afirmaciones:

(1) *B es un dominio de integridad.*
(2) *Si $\mathrm{Ker}(f)$ es un ideal maximal, entonces B es un cuerpo.*
(3) *Si B es un cuerpo, entonces $\mathrm{Im}(f)$ es un cuerpo.*
(4) *f es necesariamente inyectivo.*
(5) *f es necesariamente sobreyectivo.*
(6) *Si A es un cuerpo, entonces B es un cuerpo.*
(7) *Si B es un cuerpo, entonces A es un cuerpo.*
(8) *Si A tiene dimensión n, entonces B tiene dimensión $\leq n$.*
(9) *Si A tiene dimensión n, entonces B tiene dimensión n.*
(10) *Para cada elemento $b \in B$ existen $a_0, \ldots, a_{n-1} \in A$ tales que $a_0 + a_1 b + \cdots + a_{n-1} b^{n-1} + b^n = 0$.*

SOLUCIÓN

Capítulo VII

Espectro primo y localización

Introducción

Una de las técnicas más útiles en Álgebra Conmutativa es la de localización. Desde un punto de vista algebraico ésta permite, de forma dual al anillo cociente, estudiar los ideales (primos) contenidos en uno dado y, desde el punto de vista geométrico, permite estudiar conjuntos algebraicos en las proximidades de algunos de sus puntos o, más en general, en las proximidades de subconjuntos algebraicos irreducibles.

Se inicia el capítulo con una introducción a los anillos de fracciones, su construcción y sus propiedades elementales. En la segunda sección se aplican estos resultados al estudio de los ideales primos de anillos de polinomios, estableciendo en este caso tests de primalidad de ideales. Se cierra el capítulo con la construcciones de los módulos de fracciones y el estudio de las propiedades categóricas que se deducen de estas construcciones.

40. Localización

Sea A un anillo y $\Sigma \subseteq A$ un subconjunto cerrado para la multiplicación y conteniendo al elemento uno, i.e., **multiplicativamente cerrado**. Suponemos además que $0 \notin \Sigma$. Se considera el producto cartesiano $A \times \Sigma$, y en él se define una relación de equivalencia

$$(a_1, s_1) \equiv (a_2, s_2) \text{ si, y sólo si, existe } t \in \Sigma \text{ tal que } (a_1 s_2 - a_2 s_1)t = 0. \qquad \text{(VII.1)}$$

Lema. 40.1.
Sea A un anillo y Σ un subconjunto multiplicativo, entonces $(A \times \Sigma)/\equiv$, con operaciones definidas por:

$$\overline{(a_1, s_1)} + \overline{(a_2, s_2)} = \overline{(a_1 s_2 + a_2 s_1, s_1 s_2)},$$
$$\overline{(a_1, s_1)}\,\overline{(a_2, s_2)} = \overline{(a_1 a_2, s_1 s_2)}$$

y elemento uno igual a $\overline{(1,1)}$, es un anillo conmutativo y la aplicación $\lambda_{\Sigma,A} : A \to (A \times \Sigma)/\equiv$, definida por $\lambda_{\Sigma,A}(a) = \overline{(a,1)}$ es un homomorfismo de anillos.

Para simplificar la notación representamos a $(A \times \Sigma)/\equiv$ simplemente por $\Sigma^{-1}A$ y lo llamamos el **anillo de fracciones** de A respecto a Σ. El elemento $\overline{(a,s)}$ se representa por $\frac{a}{s}$. La aplicación $\lambda_{\Sigma,A}$ se representa, abreviadamente, por λ.

DEMOSTRACIÓN. La operación suma está bien definida. Sea $\frac{a}{b} = \frac{a'}{b'}$, por lo tanto existe $s \in \Sigma$ tal que $s(ab' - a'b) = 0$, para cada $\frac{c}{d} \in \Sigma^{-1}A$ se tiene:

$$\left(\frac{a}{b} + \frac{c}{d}\right) - \left(\frac{a'}{b'} + \frac{c}{d}\right) = \frac{ad + bc}{bd} - \frac{a'd + b'c}{b'd} = \frac{(ad + bc)b'd - (a'd + b'c)bd}{bb'd^2}.$$

Para ver que el resultado es igual a cero escribimos:

$$s[(ad + bc)b'd - (a'd + b'c)bd] = s[ab'd^2 + bb'cd - a'bd^2 - bb'cd] = s(ab' - a'b)d^2 = 0.$$

Por otro lado se tiene

$$\left(\frac{a}{b} \times \frac{c}{d}\right) - \left(\frac{a'}{b'} \times \frac{c}{d}\right) = \frac{ac}{bd} - \frac{a'c}{b'd} = \frac{acb'd - a'cbd}{bb'd^2}.$$

Para ver que el resultado es igual a cero escribimos:

$$s[acb'd - a'cbd] = s(ab' - a'b)cd = 0.$$

Las propiedades aritméticas de la suma y el producto son directas y se dejan como ejercicio para el lector. □

Observaciones. 40.2.

(1) Si $0 \in \Sigma$, entonces el anillo $\Sigma^{-1}A$ es el anillo trivial, esto es, todos los elementos son iguales a cero. Por lo tanto vamos a suponer, como señalamos al principio y si no se especifica lo contrario, que Σ no contiene al elemento cero.

(2) El sentido de incluir t en la definición de la relación de equivalencia en (VII.1) es para asegurar que una fracción a/s es la fracción cero si, y solo si, existe $t \in \Sigma$ tal que $at = 0$, y es necesaria ya que el anillo A no tiene que ser necesariamente un dominio de integridad. Observa que si no incluimos t es la definición de la relación de equivalencia y $0 \neq a \in A$ verifica $as' = 0$ para algún $s' \in \Sigma$, entonces

$$\frac{a}{1} = \frac{as'}{s'} = \frac{0}{s'} = \frac{0}{1},$$

lo que sería una contradicción, ya que entonces debería ocurrir que $a = 0$.

Lema. 40.3.
Sea A un anillo y Σ un subconjunto multiplicativo. Se verifica

$$\mathrm{Ker}(\lambda_{\Sigma,A}) = \{a \in A \mid \exists s \in \Sigma \text{ tal que } as = 0\}.$$

En particular son equivalentes los siguientes enunciados:

(a) $\lambda_{\Sigma,A} : A \to \Sigma^{-1}A$ es inyectivo.
(b) Σ no contiene divisores de cero.

DEMOSTRACIÓN. La descripción del núcleo es consecuencia directa de la definición de la relación de equivalencia. Para la equivalencia tenemos:
(a) $\Rightarrow$ (b). Supongamos que λ es inyectivo y que $s \in \Sigma$ es un divisor de cero, entonces existe $0 \neq x \in A$ tal que $sx = 0$, y por tanto $\lambda(x) = 0$, lo que es una contradicción.
(b) $\Rightarrow$ (a). Si $\lambda(x) = 0$, entonces $x/1 = 0/1$, y existe $s \in \Sigma$ tal que $sx = 0$. Por tanto s es un divisor de cero, lo que es una contradicción. □

Teorema. 40.4. (Propiedad universal del anillo de fracciones.)
Dado un anillo conmutativo A y un subconjunto multiplicativo Σ, para cada homomorfismo de anillos conmutativos $f : A \to B$ tal que para cada $s \in \Sigma$ se verifica que $f(s) \in B$ es invertible, existe un único homomorfismo de anillos $f' : \Sigma^{-1}A \to B$ tal que $f = f' \circ \lambda_{\Sigma,A}$.

$$\begin{array}{ccc} A & \xrightarrow{\lambda_{\Sigma,A}} & \Sigma^{-1}A \\ & {\scriptstyle f}\searrow & \swarrow{\scriptstyle f'} \\ & B & \end{array}$$

DEMOSTRACIÓN. En caso de existir f' estaría definida $f'(a/s) = f(a)f(s)^{-1}$, de aquí se deduce la unicidad. Se deja al lector comprobar que así definida f' verifica las condiciones del enunciado. □

Corolario. 40.5.
Sea A un anillo conmutativo, Σ un subconjunto multiplicativo y $f : A \longrightarrow B$ un homomorfismo de anillos verificando:

(1) Para cada $s \in \Sigma$ se tiene que $f(s)$ es una unidad en B;
(2) Si $f(a) = 0$, entonces existe $s \in \Sigma$ tal que $sa = 0$;
(3) Para cada $b \in B$ existen $a \in A$ y $s \in \Sigma$ tales que $b = f(a)f(s)^{-1}$.

Entonces existe un único isomorfismo $f' : \Sigma^{-1}A \to B$ tal que $f = \lambda_{\Sigma,A} \circ f'$.

$$\begin{array}{ccc} A & \xrightarrow{\lambda_{\Sigma,A}} & \Sigma^{-1}A \\ & {\scriptstyle f}\searrow & \swarrow{\scriptstyle f'} \\ & B & \end{array}$$

DEMOSTRACIÓN. Basta comprobar que al verificar las condiciones del enunciado el homomorfismo f' del Teorema (40.4.) es un isomorfismo. Es inyectiva, ya que si $f'(a/s) = 0$, entonces $f(a) = 0$ y existe $t \in \Sigma$ tal que $at = 0$, luego $a/s = 0/1$. Es sobreyectiva, ya que para cada $b \in B$ existen $a \in A$ y $s \in \Sigma$ tales que $b = f(a)f(s)^{-1} = f'(a/s)$. □

Las tres propiedades anteriores caracterizan al anillo de fracciones de A respecto a Σ.

Ejemplo. 40.6.
Sea A un anillo y Σ un conjunto de unidades de A, entonces $\Sigma^{-1}A \cong A$.

Ejemplo. 40.7.
Sea A un anillo conmutativo y $\mathfrak{p}$ un ideal primo de A, entonces $A \setminus \mathfrak{p}$ es un subconjunto multiplicativo. El anillo de fracciones $\Sigma^{-1}A$ se representa por $A_{\mathfrak{p}}$.

Lema. 40.8.
Con la notación anterior se tiene que $A_{\mathfrak{p}}$ es un anillo local con ideal maximal

$$\mathfrak{p}A_{\mathfrak{p}} = \{a/s \in A_{\mathfrak{p}} \mid \ a \in \mathfrak{p}, \ s \in A \setminus \mathfrak{p}\}.$$

DEMOSTRACIÓN. Es claro que $\mathfrak{p}A_{\mathfrak{p}} = \mathfrak{p}^e = \{a/s \in A_{\mathfrak{p}} \mid \ a \in \mathfrak{p}, s \in A \setminus \mathfrak{p}\}$ es un ideal de $A_{\mathfrak{p}}$. Además, si $b/1 \notin \mathfrak{p}A_{\mathfrak{p}}$, entonces $b \notin \mathfrak{p}$, luego $b \in A \setminus \mathfrak{p}$ y $b/1$ es invertible. □

Ejemplo. 40.9.
Sea A un anillo conmutativo y $\Sigma_0 = \Sigma_0(A) = \mathrm{Reg}(A)$, el conjunto de los elementos regulares de A. El anillo de fracciones $\Sigma_0^{-1}A$ se llama el **anillo total de fracciones** de A.
Cuando A es un dominio de integridad, entonces $\Sigma_0 = A \setminus \{0\}$ y el anillo de fracciones es un cuerpo, lo llamamos el **cuerpo de fracciones** de A.
Como consecuencia del Lema (40.3.), para cada subconjunto multiplicativo Σ si $\lambda_{\Sigma,A} : A \longrightarrow \Sigma^{-1}A$ es inyectivo, entonces $\Sigma \subseteq \Sigma_0$, y es claro que el anillo total de fracciones de A es el mayor anillo de fracciones de A en el que A está incluido como un subanillo.

Ejemplo. 40.10.
Dado un anillo conmutativo A y un elemento $a \in A$, el conjunto $\Sigma = \{a^n \mid n \in \mathbb{N}\}$ es multiplicativo. El anillo de fracciones $\Sigma^{-1}A$ se representa por A_a, y está formado por todas las fracciones que tienen como denominador una potencia de a. Observar que si a es nilpotente, entonces $0 \in \Sigma$ y el anillo de fracciones A_a se reduce a 0.

Ideales primos

Lema. 40.11. (Teorema de Krull.)
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo (que no contiene a cero), se verifica:
(1) Cada ideal $\mathfrak{a}$, maximal entre los ideales que verifican $\mathfrak{a} \cap \Sigma = \varnothing$, es un ideal primo.
(2) Para cada ideal $\mathfrak{a}$ tal que $\mathfrak{a} \cap \Sigma = \varnothing$, existe un ideal $\mathfrak{p}$ verificando $\mathfrak{p} \supseteq \mathfrak{a}$ y maximal entre los que no cortan a Σ. En particular $\mathfrak{p}$ es un ideal primo.
(3) Tomando $\mathfrak{a} = 0$ resulta que existe un ideal primo $\mathfrak{p}$ que es maximal entre los ideales que no cortan a Σ.

DEMOSTRACIÓN. Dado Σ definimos $\Gamma = \{\mathfrak{b} \mid \mathfrak{p} \cap \Sigma = \varnothing\}$.
(1). Es fácil ver que cada elemento maximal de Γ es un ideal primo.
(2). Definimos $\Lambda = \{\mathfrak{p} \mid \mathfrak{b} \supseteq \mathfrak{a}, \text{ y } \mathfrak{b} \cap \Sigma = \varnothing\}$, ya que $\mathfrak{a} \in \Lambda$ podemos aplicar el lema de Zorn para obtener el resultado.
(3). Ya que $0 \in \Gamma$, éste es no vacío. Además es inductivo. Aplicando el Lema de Zorn existen en Γ elementos maximales. □

Corolario. 40.12.
Sea A un anillo conmutativo, entonces A tiene ideales maximales y cada ideal propio está contenido en un ideal maximal.

A continuación, suponiendo probado el anterior Corolario, ver por ejemplo el Lema (4.9.), se puede hacer la siguiente demostración del Lema de Krull.

DEMOSTRACIÓN. [Otra demostración del Lema de Krull.] Se considera el homomorfismo $\lambda : A \longrightarrow \Sigma^{-1}A$. En $\Sigma^{-1}A$ tomamos un ideal maximal $\mathfrak{m}$. Finalmente tomamos $\mathfrak{p} := \lambda^{-1}(\mathfrak{m})$, que es un ideal primo de A que es maximal entre los que verifican $\mathfrak{p} \cap \Sigma = \varnothing$. □

Subconjuntos saturados

Sea A un anillo conmutativo, un subconjunto multiplicativo se llama **saturado** si verifica:

$$ab \in \Sigma \text{ implica } a \in \Sigma \text{ y } b \in \Sigma \text{ para cualesquiera } a, b \in A$$

el ejemplo típico de subconjunto multiplicativo saturado es el complemento de un ideal primo. Es claro que la intersección de subconjuntos multiplicativos saturados también lo es, luego para cada subconjunto multiplicativo podemos considerar su **clausura saturada**, esto es, la intersección de los subconjuntos multiplicativos saturados que lo contienen; lo representamos por $\overline{\Sigma}$. La descripción de la clausura saturada de Σ es:

$$\overline{\Sigma} = \{a \in A \mid \text{ existe } b \in A \text{ con } ab \in \Sigma\}.$$

En efecto, es claro que $\overline{\Sigma}$, así definido, es un subconjunto multiplicativo saturado que contiene a Σ. Para ver que es saturado, sean $a_1a_2 \in \overline{\Sigma}$, existe $b \in A$ tal que $(a_1a_2)b \in \Sigma$, de la igualdad $(a_1a_2)b = a_1(a_2b) = a_2(a_1b)$ se tiene que $a_1, a_2 \in \overline{\Sigma}$.

En este caso se tiene un isomorfismo $\Sigma^{-1}A \cong \overline{\Sigma}^{-1}A$. Ver Ejercicio (43.32.).

Otra descripción de $\overline{\Sigma}$ se obtiene como consecuencia del Teorema de Krull.

Lema. 40.13.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo, entonces

$$\overline{\Sigma} = \cap\{A \setminus \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(A), \ \mathfrak{p} \cap \Sigma = \varnothing\}$$

DEMOSTRACIÓN. Dado Σ definimos

$$\Sigma_s = \cap\{A \setminus \mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(A), \ \mathfrak{p} \cap \Sigma = \varnothing\}.$$

Es claro que $\Sigma \subseteq \Sigma_s$ y que Σ_s es saturado ya que es intersección de subconjuntos saturados. Como consecuencia $\overline{\Sigma} \subseteq \Sigma_s$. Sea ahora $x \in \Sigma_s \setminus \overline{\Sigma}$, entonces para cada ideal primo $\mathfrak{p}$ tal que $\mathfrak{p} \cap \Sigma = \varnothing$ se tiene $x \notin \mathfrak{p}$. Por otro lado $x \notin \overline{\Sigma}$, y como $\overline{\Sigma}$ es saturado, para cada $a \in A$ se tiene $ax \notin \overline{\Sigma}$, esto es, $Ax \cap \overline{\Sigma} = \varnothing$. Existe un ideal $\mathfrak{q}$ maximal entre los que contienen a Ax y no cortan a $\overline{\Sigma}$. Es claro que $\mathfrak{q}$ es un ideal primo que no corta a Σ y que por tanto no puede contener a x, llegando así a una contradicción. □

Ver Ejercicio (43.31.)

Observa que se tiene $\overline{\Sigma} = A \setminus (\cup\{\mathfrak{p} \mid \mathfrak{p} \cap \Sigma = \varnothing\})$. Por lo tanto todo subconjunto multiplicativo saturado es un complemento de una unión de ideales primos.

Ejemplo. 40.14.
Sea A un anillo conmutativo, como $\mathcal{U}(A)$, el conjunto de las unidades de A, es un conjunto multiplicativo saturado, entonces $A\setminus\mathcal{U}(A)$ es una unión de ideales primos, en concreto de todos los ideales maximales de A.

Ejemplo. 40.15.
Sea A un anillo conmutativo y $\operatorname{Reg}(A)=\Sigma_0$, el conjunto de los elementos regulares, entonces $A\setminus\operatorname{Reg}(A)$ es el conjunto de los divisores de cero. Como $\operatorname{Reg}(A)$ es un subconjunto multiplicativo saturado, tenemos que el conjunto de los divisores de cero es una unión de ideales primos.

A los ideales maximales, entre los que están contenidos en el conjunto de los divisores de cero, los llamamos **ideales maximales de divisores de cero** de A.

Veamos otra aplicación. Sea M un A–módulo, llamamos $\operatorname{Div}(M)=\{a\in A \mid \text{ existe } 0\neq m\in M \text{ tal que } am=0\}$ y $\operatorname{Reg}(M)=A\setminus\operatorname{Div}(M)$.

Lema. 40.16.
Con la notación anterior tenemos que $\operatorname{Reg}(M)$ *es un subconjunto multiplicativo saturado y por tanto* $\operatorname{Div}(M)$ *es una unión de ideales primos.*

DEMOSTRACIÓN. Es claro que $\operatorname{Reg}(M)$ es un subconjunto multiplicativo saturado. □

Los ideales primos contenidos en $\operatorname{Div}(M)$ se llaman **ideales primos** de M y los maximales se llaman **ideales primos maximales** de M.

Proposición. 40.17.
Sea A un anillo conmutativo y Σ, Γ subconjuntos multiplicativos tales que $\Sigma\subseteq\Gamma$, entonces existe un único homomorfismo de anillos f tal que $\lambda_{\Gamma,A}=f\circ\lambda_{\Sigma,A}$, ver el siguiente diagrama para las notaciones.

$$\begin{array}{ccc} A & \xrightarrow{\lambda_{\Sigma,A}} & \Sigma^{-1}A \\ & {\scriptstyle\lambda_{\Gamma,A}}\searrow \quad \swarrow {\scriptstyle f} & \\ & \Gamma^{-1}A & \end{array}$$

Además son equivalentes las siguientes propiedades:

(a) f es un isomorfismo.
(b) Un ideal primo $\mathfrak{p}$ de A no corta a Σ si, y solo si, no corta a Γ.
(c) Las saturaciones de Σ y Γ son iguales.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si $\mathfrak{p}\cap\Gamma\neq\varnothing$, existe $s\in\mathfrak{p}\cap\Gamma$, como $\lambda_{\Sigma,A}(s)=f^{-1}\circ\lambda_{\Gamma,A}(s)$ es invertible en $\Sigma^{-1}A$, entonces $s\in\Sigma$ y tenemos $\mathfrak{p}\cap\Sigma\neq\varnothing$.

(b) $\Rightarrow$ (c). Es evidente de la caracterización de la saturación de Σ como intersección de los ideales primos que no cortan a Σ.
(c) $\Rightarrow$ (a). Como existe un isomorfismo $\Sigma^{-1}A \cong \overline{\Sigma}^{-1}A$, ver Ejercicio (43.32.), el resultado es evidente.

□

Extensión y contracción de ideales. Anillos locales

Sea A un anillo conmutativo, Σ un subconjunto multiplicativo y $\lambda_{\Sigma,A} : A \longrightarrow \Sigma^{-1}A$ el homomorfismo canónico. Para cada ideal $\mathfrak{a}$ de A se tiene

$$\mathfrak{a}^e = \lambda(\mathfrak{a})\Sigma^{-1}A = \mathfrak{a}\Sigma^{-1}A = \{a/s \in \Sigma^{-1}A \mid a \in \mathfrak{a}, s \in \Sigma\} = \Sigma^{-1}\mathfrak{a}.$$

Si $\mathfrak{b}$ es un ideal de $\Sigma^{-1}A$, entonces

$$\lambda^{-1}(\mathfrak{b}) = \{a \in A \mid a/1 \in \mathfrak{b}\} = \mathfrak{b}^c.$$

En general se verifica $\mathfrak{b} = \mathfrak{b}^{ce}$ y $\mathfrak{a} \subsetneqq \mathfrak{a}^{ec}$. Para analizar la última inclusión llamamos a $\mathfrak{a}^{ec}$ la Σ–**saturación** de $\mathfrak{a}$, y la representamos por $\operatorname{Sat}_\Sigma(\mathfrak{a})$. Es claro que

$$\mathfrak{a}^{ec} = \{a \in A \mid \text{ existe } s \in \Sigma \text{ tal que } sa \in \mathfrak{a}\}.$$

Observa que $0^{ec} = \operatorname{Ker}(\lambda_{\Sigma,A} = \{a \in A \mid \text{ existe } s \in \Sigma \text{ tal que } sa = 0\}$.

Ejemplo. 40.18.
Se considera el anillo $\mathbb{Z}$ y el subconjunto multiplicativo $\Sigma = \mathbb{Z}\setminus\{0\}$. Si $\mathfrak{a} = 2\mathbb{Z}$, entonces $\mathfrak{a}^e = 2\mathbb{Z}\mathbb{Q} = \mathbb{Q}$ y es claro que $\mathfrak{a} \subsetneqq \mathfrak{a}^{ec} = \mathbb{Z}$.

Proposición. 40.19.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo, existe una biyección que conserva el orden entre los ideales de $\Sigma^{-1}A$ y los ideales Σ–saturados de A. Además para cada ideal $\mathfrak{a}$ de A se verifica $\mathfrak{a}^{ec} = A$ si, y sólo si, $\mathfrak{a} \cap \Sigma \neq \varnothing$.
En particular existe una correspondencia biyectiva entre los ideales primos de $\Sigma^{-1}A$ y los ideales primos de A que no cortan a Σ.

DEMOSTRACIÓN. Es clara la biyección entre los ideales de $\Sigma^{-1}A$ y los ideales Σ–saturados de A, así como el que $\mathfrak{a}^e = \Sigma^{-1}S$ si y sólo si $\mathfrak{a} \cap \Sigma \neq \varnothing$. Por otro lado, si $\mathfrak{p}$ es un ideal primo de A que no corta a Σ, entonces $\mathfrak{p}$ es Σ–saturado, lo que prueba la biyección señalada. Vamos a ver que si $\mathfrak{p}$ es primo y $\mathfrak{p} \cap \Sigma = \varnothing$, entonces $\mathfrak{p} = \mathfrak{p}^{ec}$. Si $x \in \mathfrak{p}^{ec}$, existe $s \in \Sigma$ tal que $xs \in \mathfrak{p}$, y como $\mathfrak{p}$ es primo y $s \notin \mathfrak{p}$, se tiene $x \in \mathfrak{p}$. □

Proposición. 40.20.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo, entonces Σ^{-1} es una función creciente en el conjunto de los ideales que conmuta con las siguientes operaciones de ideales:

(1) Sumas.
(2) Productos.
(3) Intersecciones finitas.
(4) Radicales.

DEMOSTRACIÓN. Es claro que si $\mathfrak{a} \subseteq \mathfrak{b}$, entonces $\Sigma^{-1}\mathfrak{a} \subseteq \Sigma^{-1}\mathfrak{b}$.
Se tiene $\sum_{\lambda\in\Lambda} \Sigma^{-1}\mathfrak{a} \subseteq \Sigma(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda)$, y si $a/1 \in \Sigma(\sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda)$, existe $s \in \Sigma$ tal que $as \in \sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$; si $as = \sum_\lambda a_\lambda \in \sum_{\lambda\in\Lambda} \mathfrak{a}_\lambda$, de soporte finito, entonces $a/1 = as/s = \sum_\lambda a_\lambda/s \in \sum_{\lambda\in\Lambda} \Sigma^{-1}\mathfrak{a}_\lambda$, y tenemos la igualdad.
Basta probar que $\Sigma^{-1}(\mathfrak{a}\mathfrak{b}) = (\Sigma^{-1}\mathfrak{a})(\Sigma^{-1}\mathfrak{b})$.
Como $\Sigma^{-1}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \Sigma^{-1}\mathfrak{a}, \Sigma^{-1}\mathfrak{b}$, se tiene $\Sigma^{-1}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \Sigma^{-1}\mathfrak{a} \cap \Sigma^{-1}\mathfrak{b}$. Por otro lado, si $a/1 \in \Sigma^{-1}\mathfrak{a} \cap \Sigma^{-1}\mathfrak{b}$, existe $s \in \Sigma$ tal que $as \in \mathfrak{a}, \mathfrak{b}$, luego $a/1 = as/s \in \Sigma^{-1}(\mathfrak{a} \cap \mathfrak{b})$.
Si $a/1 \in \operatorname{rad}(\Sigma^{-1}\mathfrak{a})$, existe $n \in \mathbb{N}$ tal que $a^n/1 \in \Sigma^{-1}\mathfrak{a}$, y existe $s \in \Sigma$ tal que $a^n s \in \mathfrak{a}$, luego $a^n s^n \in \mathfrak{a}$ y $as \in \operatorname{rad}(\mathfrak{a})$, por lo tanto $a/1 = as/s \in \Sigma^{-1}\mathfrak{a}$. Por otro lado, si $a/1 \in \Sigma^{-1}\mathfrak{a}$ existe $s \in \Sigma$ tal que $as \in \operatorname{rad}(\mathfrak{a})$ y existe $n \in \mathbb{N}$ al que $a^n s^n \in \mathfrak{a}$, entonces $a^n/1 = a^n s^n/s^n \in \Sigma^{-1}\mathfrak{a}$, y $a/1 \in \operatorname{rad}(\Sigma^{-1}\mathfrak{a})$.
□

Para intersecciones arbitrarias el resultado no es cierto, como prueba el siguiente ejemplo.

Ejemplo. 40.21.
Considera el anillo $A = \mathbb{Z}$, y para cada $n \in \mathbb{N}^*$ el ideal $\mathfrak{a}_n = n\mathbb{Z}$. Tomamos $\Sigma = \mathbb{Z} \setminus \{0\}$. Se verifica:

$$\Sigma^{-1}\left(\cap_n \mathfrak{a}_n\right) = \Sigma^{-1}0 = 0.$$

Por otro lado

$$\cap_n \left(\Sigma^{-1}\mathfrak{a}_n\right) = \cap_n \mathbb{Q} = \mathbb{Q}.$$

Aunque Σ^{-1} no conmuta con intersecciones infinitas, como consecuencia de la conmutación de Σ^{-1} y el radical de ideales se tiene el siguiente resultado:

Corolario. 40.22.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo, se verifica: $\operatorname{Nil}(\Sigma^{-1}A) = \Sigma^{-1}\operatorname{Nil}(A)$.

DEMOSTRACIÓN. Es claro que

$$\Sigma^{-1}\operatorname{Nil}(A) = \Sigma^{-1}(\cap\{\mathfrak{p} \mid \mathfrak{p} \text{ primo en } A\}) \subseteq \cap\{\Sigma^{-1}\mathfrak{p} \mid \mathfrak{p} \text{ primo en } A\} = \operatorname{Nil}(\Sigma^{-1}A).$$

Por otro lado, si $\frac{a}{s} \in \operatorname{Nil}(\Sigma^{-1}A)$, existe $n \in \mathbb{N}$ tal que $\left(\frac{a}{s}\right)^n = 0$, y por tanto existe $t \in \Sigma$ tal que $ta^n = 0$. Entonces $(ta)^n = 0$ y $ta \in \operatorname{Nil}(A)$. En consecuencia $\frac{a}{s} = \frac{ta}{ts} \in \Sigma^{-1}\operatorname{Nil}(A)$. □

Si $\mathfrak{p}$ es un ideal primo de un anillo A, el localizado $A_\mathfrak{p}$ tiene un único ideal maximal, ver Proposición (40.19.). Por lo tanto es un **anillo local**, y existe una biyección entre los ideales primos de $A_\mathfrak{p}$ y los ideales primos de A contenidos en $\mathfrak{p}$. Como consecuencia, si $\mathfrak{p}$ es un ideal primo minimal (no contiene a ningún otro ideal primo) de A, entonces $A_\mathfrak{p}$ es un anillo con un único ideal primo.

La siguiente es una descripción del anillo de fracciones, en el caso particular de un dominio, en el sentido señalado en el Ejemplo (40.9.).

Proposición. 40.23.
Sea D un dominio de integridad con cuerpo de fracciones K, entonces

(1) cada anillo de fracciones de $\Sigma^{-1}D$ de D es un subanillo de K y
(2) se verifica: $D = \cap\{D_\mathfrak{m} \mid \mathfrak{m} \in \operatorname{Max}(D)\}$.

DEMOSTRACIÓN. Dado un subconjunto multiplicativo $\Sigma \subseteq D$ se tiene $\Sigma \subseteq D \setminus \{0\}$, luego $D \subseteq \Sigma^{-1}A \subseteq K$.

Se tiene entonces $D \subseteq \cap_\mathfrak{m} D_\mathfrak{m}$. Por otro lado, se $x \in \cap_\mathfrak{m} D_\mathfrak{m}$, entonces para cada $x \in \cap_\mathfrak{m} A_\mathfrak{m}$ existen $a_x \in A$ y $s_x \in A \setminus \mathfrak{m}$ tales que $x = a_x/s_x$. Como consecuencia $xs_x = a_x \in A$. Entonces el ideal $A : x = \{a \in A \mid xa \in A\}$ no está contenido en ningún ideal maximal $\mathfrak{m}$, y por lo tanto $A : x = A$, esto es, $x \in A$. □

Ver Ejercicio (43.52.)

Observación. 40.24.
Ya que para cada ideal primo $\mathfrak{p}$ de un anillo A existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{p} \subseteq \mathfrak{m}$, entonces existe un homomorfismo $A_\mathfrak{m} \to A_\mathfrak{p}$. Si A un dominio, éste es inyectivo y podemos, en la anterior intersección, sustituir el conjunto de los ideales maximales por el conjunto de los ideales primos.

Anillos noetherianos

Lema. 40.25.
Sea A un anillo noetheriano y $\Sigma \subseteq A$ un subconjunto multiplicativo, entonces $\Sigma^{-1}A$ es un anillo noetheriano.

DEMOSTRACIÓN. Es consecuencia de la Proposition (40.20.). □

Ver Ejercicio (43.43.)

Lema. 40.26.
Si A es un anillo, $\mathfrak{a} \subseteq A$ un ideal y $\Sigma \subseteq A$ un subconjunto multiplicativo, se verifica:
(1) Si $\mathfrak{a} = (a_1, \ldots, a_t)$, entonces $\Sigma^{-1}\mathfrak{a} := \mathfrak{a}\Sigma^{-1}A = (\frac{a_1}{1}, \ldots, \frac{a_t}{1})$.
(2) Si $\mathfrak{a}$ es principal, entonces $\mathfrak{a}\Sigma^{-1}A$ es principal.

DEMOSTRACIÓN. □

Ver Ejercicio (43.43.)

Ideales primarios

Ya conocemos que los ideales primos son ideales saturados. Vamos a introducir un nuevo tipo de ideales saturados: *los ideales primarios*.
Sea A un anillo conmutativo. Un ideal $\mathfrak{a}$ se llama **primario** si verifica:

$$ab \in \mathfrak{a} \text{ y } a \notin \mathfrak{a}, \text{ entonces existe } n \in \mathbb{N} \text{ tal que } b^n \in \mathfrak{a}.$$

Como consecuencia de la definición, si $\mathfrak{a}$ es un ideal primario, entonces $\operatorname{rad}(\mathfrak{a})$ es un ideal primo, sea $\mathfrak{p}$, entonces $\mathfrak{a}$ se llama **$\mathfrak{p}$–primario**.

Proposición. 40.27.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo, se verifica:
(1) Si $\mathfrak{p} \in \operatorname{Spec}(A)$, $\mathfrak{p} \cap \Sigma = \varnothing$ y $\mathfrak{a}$ un ideal $\mathfrak{p}$–primario, entonces $\mathfrak{a}$ es Σ–saturado (también podemos quedarnos con la condición $\mathfrak{a} \cap \Sigma = \varnothing$);
(2) Si $\mathfrak{p} \in \operatorname{Spec}(A)$, $\mathfrak{p} \cap \Sigma \neq \varnothing$ y $\mathfrak{a}$ un ideal $\mathfrak{p}$–primario, entonces $\Sigma^{-1}\mathfrak{a} = \Sigma^{-1}A$;
(3) Existe una correspondencia biyectiva entre ideales primarios de $\Sigma^{-1}A$ e ideales primarios de A que no cortan a Σ.

DEMOSTRACIÓN. (1). Como $\mathfrak{p} \cap \Sigma = \varnothing$, resulta que $\Sigma \subseteq A \setminus \mathfrak{p}$, y por tanto basta comprobar que si $as \in \mathfrak{a}$, con $s \notin \mathfrak{p}$, entonces $a \in \mathfrak{a}$. En efecto, si $a \notin \mathfrak{a}$, existe $n \in \mathbb{N}$ tal que $s^n \in \mathfrak{a} \subseteq \mathfrak{p}$, lo que es una contradicción.
(2). En este caso basta comprobar que $\mathfrak{a} \cap \Sigma \neq \varnothing$. Si $\mathfrak{p} \cap \Sigma \neq \varnothing$, para cada $s \in \mathfrak{p} \cap \Sigma$ existe $n \in \mathbb{N}$ tal que $s^n \in \mathfrak{a}$, luego $s^n \in \mathfrak{a} \cap \Sigma$.
(3). Dado $\mathfrak{a}$ un ideal primario que no corta a Σ basta ver que $\Sigma^{-1}\mathfrak{a}$ es un ideal primario en $\Sigma^{-1}A$. Sean $(a/1)(b/1) \in \Sigma^{-1}\mathfrak{a}$, entonces $ab/1 \in \Sigma^{-1}\mathfrak{a}$ y tenemos $ab \in \mathfrak{a}$ por ser $\mathfrak{a}$ un ideal Σ–saturado. Entonces $a \in \mathfrak{a}$ o existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{a}$. Por tanto tenemos $a/1 \in \Sigma^{-1}\mathfrak{a}$ o existe $n \in \mathbb{N}$ tal que $(b/1)^n \in \Sigma^{-1}\mathfrak{a}$. Recíprocamente, si $\mathfrak{q} \subseteq \Sigma^{-1}A$ es primario y $ab \in \mathfrak{q}^c$, se tiene $(ab)/1 \in \mathfrak{q}$, luego $a/1 \in \mathfrak{q}$ o existe $n \in \mathbb{N}$ tal que $(b/1)^n \in \mathfrak{q}$. Entonces se tiene $a \in \mathfrak{q}^c$ o existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{q}^c$. □

41. Ideales primos en anillos de polinomios

Dado un anillo A estamos interesados en determinar si un ideal dado de $A[X]$ es primo. Para esto hacemos la siguiente observación: *Dado un ideal primo $\mathfrak{p}$ de $A[X]$ se tienen los siguientes resultados*:

(1) $\mathfrak{p} \cap A \subseteq A$ *es un ideal primo.*

Llamamos $B := A/(\mathfrak{p} \cap A)$. Como B es un dominio, sea F su cuerpo de fracciones. Se verifica que $F[X]$ es el anillo de fracciones de $B[X]$ con respecto al subconjunto multiplicativo $\Sigma = B \setminus \{0\} \subseteq B[X]$. Existe un homomorfismo de anillos:

$$A[X] \xrightarrow{\quad\alpha\quad} \frac{A}{(\mathfrak{p} \cap A)}[X] = B[X] \xrightarrow{\quad\beta\quad} F[X],$$

donde α es la proyección canónica y β la inclusión en el localizado.
Se tiene $\operatorname{Ker}(\alpha) = (\mathfrak{p} \cap A)[X] \subseteq \mathfrak{p}$, luego $\alpha(\mathfrak{p})$ es un ideal primo de $B[X]$. Como $\alpha(\mathfrak{p}) \cap \Sigma = \varnothing$, ya que si $b = a + (\mathfrak{p} \cap A) \in \alpha(\mathfrak{p}) \cap \Sigma$, existe $p \in \mathfrak{p}$ tal que $\alpha(p) = b = \alpha(a)$, luego $p - a \in \operatorname{Ker}(\alpha) \subseteq \mathfrak{p}$, y por tanto $a \in \mathfrak{p} \cap A$ y $b = 0$, lo que es una contradicción, tenemos:

(2) $\alpha(\mathfrak{p})^e := \beta(\alpha(\mathfrak{p}))F[X]$ *es un ideal primo de* $F[X]$ y

(3) *el ideal* $\alpha(\mathfrak{p})$ *es* Σ*–saturado en* $B[X]$.

Esto último es consecuencia de que $\alpha(\mathfrak{p})$ es un ideal primo que $\alpha(\mathfrak{p}) \cap \Sigma = \varnothing$.
Vamos a probar la siguiente proposición:

Proposición. 41.1.
En la situación anterior un ideal $\mathfrak{p}$ de $A[X]$ es un ideal primo si y solo si se verifica:
(1) $\mathfrak{p} \cap A$ es un ideal primo de A.
(2) $\alpha(\mathfrak{p})^e$ es un ideal primo de $F[X]$.
(3) $\alpha(\mathfrak{p})$ es un ideal Σ–saturado de $B[X]$.

DEMOSTRACIÓN. Ya hemos probado la condición necesaria. Veamos la condición suficiente. Dados $f, g \in A[X]$ tales que $fg \in \mathfrak{p}$, aplicando $\beta \circ \alpha : A[X] \longrightarrow B[X] \longrightarrow F[X]$ tenemos $(\beta \circ \alpha)(f)(\beta \circ \alpha)(g) \in \alpha(\mathfrak{p})^e$. Entonces $(\beta\circ\alpha)(f) \in \alpha(\mathfrak{p})^e$ o $(\beta\circ\alpha)(g) \in \alpha(\mathfrak{p})^e$. Supongamos que $(\beta\circ\alpha)(f) \in \alpha(\mathfrak{p})^e$, como $\alpha(\mathfrak{p})$ es Σ–saturado se tiene $\alpha(f) \in \alpha(\mathfrak{p})$, y existe $p \in \mathfrak{p}$ tal que $\alpha(f) = \alpha(p)$, esto es, $f - p \in \operatorname{Ker}(\alpha) \subseteq \mathfrak{p}$, luego $f \in \mathfrak{p}$. □

Ejercicio. 41.2.
Veamos, como aplicación, cuales son los ideales primos de $\mathbb{Z}[X]$.

DEMOSTRACIÓN.

(1) Por un lado tenemos el ideal cero.

(2) Si $\mathfrak{p}$ es un ideal primo no nulo de $\mathbb{Z}[X]$ se tiene $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$

(2.1) Si $p = 0$, entonces $A = B = \mathbb{Z}$ y $F = \mathbb{Q}$.

$$A[X] \overset{\alpha}{=\!=\!=} B[X] \xrightarrow{\beta} F[X].$$

Por tanto $\alpha(\mathfrak{p})^e = \mathfrak{p}\mathbb{Q}[X]$ es un ideal primo no nulo de $\mathbb{Q}[X]$. Sea $\mathfrak{p}\mathbb{Q}[X] = (h)$, con $h \in \mathbb{Z}[X]$. Podemos suponer que h es un polinomio irreducible primitivo, evidentemente se tiene $\mathfrak{p} = (h)$.

(2.2) Si $p \neq 0$, entonces $A = \mathbb{Z}$, $B = F = \mathbb{Z}_p$.

$$A[X] \xrightarrow{\alpha} B[X] \overset{\beta}{=\!=\!=} F[X].$$

En este caso $\alpha(\mathfrak{p})$ es un ideal primo de $\mathbb{Z}_p[X]$.

(2.2.1) Si $\alpha(\mathfrak{p}) = 0$ tenemos $\mathfrak{p} \subseteq \operatorname{Ker}(\alpha) = (\mathfrak{p} \cap A)[X] \subseteq \mathfrak{p}$, y $\mathfrak{p} = p\mathbb{Z}[X]$.

(2.2.2) Si $\alpha(\mathfrak{p}) \neq 0$ tenemos $\alpha(\mathfrak{p}) = (h)$, siendo $h \in \mathbb{Z}_p[X]$ irreducible. En este caso existe $f \in \mathfrak{p}$ tal que $\alpha(f) = h$ y se verifica $\mathfrak{p} = (p,f)\mathbb{Z}[X]$. En efecto, si $g \in \mathfrak{p}$ tenemos $\alpha(g) = ch$, con $c \in \mathbb{Z}_p[X]$. Sea $d \in \mathbb{Z}[X]$ tal que $\alpha(d) = c$, entonces $\alpha(df) = ch = \alpha(g)$, esto es, $g - df \in \operatorname{Ker}(\alpha) \subseteq (\mathfrak{p} \cap A)[X] = p\mathbb{Z}[X]$, esto es, $g \in (p,f)\mathbb{Z}[X]$.

En resumen los ideales primos de $\mathbb{Z}[X]$ son de la forma (h), (p) ó (p,f), siendo $p \in \mathbb{Z}$ primo, $h \in \mathbb{Z}[X]$ irreducible primitivo y $f \in \mathbb{Z}[X]$ irreducible y es también irreducible módulo p. □

Ejercicio. 41.3.
Podemos completar este ejercicio determinando los ideales maximales de $\mathbb{Z}[X]$.

DEMOSTRACIÓN. (1). Es claro que los ideales primos $\mathfrak{p} = (p,f)$ son ideales maximales.
(2). Para cada entero primo p se tiene $(p) \subseteq \mathbb{Z}[X]$ no es maximal, ya que $X + (p)$ no es invertible.
(3). Veamos que para cualquier polinomio irreducible primitivo $h \in \mathbb{Z}[X]$, el ideal (h) no es un maximal. Supongamos que (h) es maximal; primero observamos que $gr(h) \geq 1$, esto es, h no es constante. A continuación tomamos $a \in \mathbb{Z}$ tal que $h(a) \neq 0, 1, -1$, y un entero primo p tal que $p \mid h(a)$. Definimos

$\alpha : \mathbb{Z}[X] \to \mathbb{Z}_p$ mediante $\alpha(X) = \overline{a} \in \mathbb{Z}_p$. Es claro que $\alpha(h) = 0$, y por tanto α factoriza por $\mathbb{Z}[X]/(h)$. Existe pues un homomorfismo $\alpha : \mathbb{Z}[X]/(h) \to \mathbb{Z}_p$. Como $\mathbb{Z}[X]/(h)$ es un cuerpo de característica cero y existe un homomorfismo de anillos a $\mathbb{Z}_p$, llegamos a una contradicción. □

Ejercicio. 41.4.
Con la notación del Ejercicio (41.2.) Prueba que para cada ideal primo $(h) \subseteq \mathbb{Z}_p[X]$ existen dos únicos ideales primos $\mathfrak{p}_1 \subsetneqq \mathfrak{p}_2$ de $\mathbb{Z}[X]$ tales que $0 = \mathfrak{p}_1 \cap \mathbb{Z} \subsetneqq \mathfrak{p}_2 \cap \mathbb{Z} = p\mathbb{Z}$ y $\alpha(\mathfrak{p}_1) = (h) = \alpha(\mathfrak{p}_2)$.

SOLUCIÓN. Ya que (h) es primo, resulta que $h \in \mathbb{Z}_p[X]$ es irreducible, entonces existe $f \in \mathbb{Z}[X]$ irreducible tal que $f \mapsto h$. Consideramos $\mathfrak{p}_1 = (f)$ y $\mathfrak{p}_2 = (p, f)$, que verifican las condiciones impuestas. La unicidad se desprende de la forma de los ideales primos de $\mathbb{Z}[X]$. □

A la hora de calcular si un ideal de $A[X]$ es primo, necesitamos un resultado técnico para comprobar la saturación de ideales.

Lema. 41.5.
Sea B un dominio de integridad con cuerpo de fracciones F, $\mathfrak{b} \subseteq B[X]$ un ideal tal que $\mathfrak{b}^e = \mathfrak{b}F[X] = (h)$, siendo $h \in B[X]$ con coeficiente líder b. Se verifica:
(1) $\mathfrak{b}^{ec} = \mathfrak{b}F[X] \cap B[X] = \mathfrak{b}B_b[X] \cap B[X] = hB_b[X] \cap B[X]$.
(2) Si $\mathfrak{c} = (\mathfrak{b}, 1 - bT)B[X, T]$, entonces $\mathfrak{b}B_b[X] \cap B[X] = \mathfrak{c} \cap B[X]$.

DEMOSTRACIÓN. (1). Ya que $B_b \subseteq F$, se tiene $hB_b[X] \subseteq \mathfrak{b}B_b[X] \subseteq hF[X] \cap B_b[X]$, y si $f \in hF[X] \cap B[X]$. Sean ax^n, bx^m los monomios líderes de f y h, respectivamente. Como $f \in hF[X]$, se tiene $n \geq m$ y tenemos

$$f - \left(\frac{a}{b}\right) X^{n-m} h \in hF[X] \cap B_b[X]$$

tiene grado menor que f. Iterando el proceso llegamos a un polinomio de grado menor que m, por lo que ha de ser igual a cero, y en consecuencia f es una combinación en B_b de múltiplos de h, esto es, $f \in hB_b[X]$, y tenemos $hF[X] \cap B_b[X] = hB_b[X]$. Al hacer la intersección con $B[X]$ tenemos:

$$\mathfrak{b}^{ec} = \mathfrak{b}F[X] \cap B[X] = hF[X] \cap B[X] = hB_b[X] \cap B[X] = \mathfrak{b}B_b[X] \cap B[X].$$

Observar que en este punto hemos reducido el problema a considerar solamente fracciones en las que los denominadores son potencia de b.

(2). Vamos a relacionar $\mathfrak{b}B_b[X] \cap B[X]$ y $\mathfrak{c} \cap B[X]$. Dado $f \in \mathfrak{b}B_b[X] \cap B[X]$ se verifica $f = hg$, siendo $g \in B_b[X]$; existe $n \in \mathbb{N}$ tal que $b^n g \in B[X]$, luego

$$f = (bT)^n f + (1 - (bT)^n) f = (T^n h(b^n g) + (1 - (bT)^n) f = hT^n (b^n g) f + (1 - (bT)^n) f \in \mathfrak{c} \cap B[X].$$

Por otro lado, sea $f \in \mathfrak{c} \cap B[X]$, se verifica $f = hg_1 + (1 - bT)g_2$, con $g_1, g_2 \in B[X, T]$, entonces, evaluando en $T = 1/b$ se tiene $f = hg_1(X, 1/b) \in hB_b[X] \cap B[X]$. □

Veamos, como aplicación cómo calcular los ideales primos en anillos de polinomios con coeficientes en un cuerpo. Sea $\mathfrak{p} \subseteq K[X_1, \ldots, X_n]$ un ideal. Llamamos $\mathfrak{p}_i = \mathfrak{p} \cap X[X_1, \ldots, X_i]$. Si $\mathfrak{p}$ es un ideal primo, entonces, necesariamente los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$ son primos; pero esta condición no es suficiente. Para encontrar una condición suficiente debemos comenzar a estudiar $\mathfrak{p}_1$, después $\mathfrak{p}_2$, y así sucesivamente hasta llegar a $\mathfrak{p}_n$. Estudiamos ese caso.

Si $\mathfrak{p}_1$ es primo tenemos $\mathfrak{p}_1 = 0$ o $\mathfrak{p}_1 = (h) \subseteq K[X_1]$, siendo h un polinomio irreducible en $K[X_1]$.

Pasamos a estudiar $\mathfrak{p}_2$. Para ilustrar este caso vamos a estudiar un caso más general, esto es, vamos a suponer que los ideales $\mathfrak{p}_1, \ldots, \mathfrak{p}_{i-1}$, $i > 1$, son primos y vamos a estudiar $\mathfrak{p}_i$. Consideramos el anillo $B = \frac{K[X_1,\ldots,X_{i-1}]}{\mathfrak{p}_{i-1}}$, y llamamos F a su cuerpo de fracciones, $\alpha : K[X_1, \ldots, X_{i-1}][X_i] \longrightarrow B[X_i]$. Estudiamos si el ideal $\alpha(\mathfrak{p}_i) \subseteq B[X_i]$ es saturado y si su extendido $\alpha(\mathfrak{p}_i)^e \subseteq F[X_i]$ es primo. Para lo segundo tenemos que ver si $\alpha(\mathfrak{p}_i)^e$ es cero o si está generado por un polinomio irreducible de $F[X_i]$. Y para lo primero tenemos que ver si $\alpha(\mathfrak{p}_i)$ coincide con su saturación $(\alpha(\mathfrak{p}_i), 1 - bT)B[X_i, T] \cap B[X_i]$. Este último estudio podemos hacerlo estudiando la intersección $(\mathfrak{p}_i, 1 - b'T)K[X_1, \ldots, X_i, T] \cap K[X_1, \ldots, X_i]$, siendo $\alpha(b') = b$, ya que:

$$\begin{array}{ccccccc}
\mathfrak{p}_i & \dashrightarrow & & & \alpha(\mathfrak{p}_i) & & \\
& \searrow & & & & \searrow & \\
& & A[X_i] & \xrightarrow{\alpha} & & & B[X_i] \\
& & \downarrow & & & & \downarrow \\
(\mathfrak{p}_i, 1 - b'T) & \dashrightarrow & & & (\alpha(\mathfrak{p}_i), 1 - bT) & & \\
& \searrow & \downarrow & & & \searrow & \downarrow \\
& & A[X, T] & \xrightarrow{\alpha'} & & & B[X, T]
\end{array}$$

Como α y α' son sobreyectivas, $\mathrm{Ker}(\alpha) \subseteq \mathfrak{p}_i$ y $\mathrm{Ker}(\alpha') \subseteq (\mathfrak{p}_i, 1 - b'T)$, resulta que $\alpha(\mathfrak{p}_i) = (\alpha(\mathfrak{p}_i), 1 - bT) \cap B[X]$ si y solo si $\mathfrak{p}_i = (\mathfrak{p}_i, 1 - b'T) \cap A[X]$. Veamos algunos ejemplos.

Ejemplo. 41.6.
Sea $\mathfrak{p} = (XZ - Y^2, YZ - X^3, Z^2 - X^2Y) \subseteq \mathbb{Q}[X, Y, Z]$. Una base de Groebner reducida para $\mathfrak{p}$, con respecto al orden lexicográfico $X > Y > Z$, es:

$$\{X^3 - YZ, X^2Y - Z^2, XY^3 - Z^3, XZ - Y^2, Y^5 - Z^4\}.$$

Definimos:

$$\begin{aligned}
&\mathfrak{p}_1 = \mathfrak{p} \cap \mathbb{Q}[Z] = 0, \\
&\mathfrak{p}_2 = \mathfrak{p} \cap \mathbb{Q}[Y, Z] = (Y^5 - Z^4), \\
&\mathfrak{p}_3 = \mathfrak{p} = (X^3 - YZ, X^2Y - Z^2, XY^3 - Z^3, XZ - Y^2, Y^5 - Z^4)
\end{aligned}$$

(Esto es consecuencia de la teoría de la eliminación.)

(1) Es claro que $\mathfrak{p}_1 \subseteq \mathbb{Q}[Z]$ es un ideal primo.

(2) En el caso de $\mathfrak{p}_2 \subseteq \mathbb{Q}[Y,Z]$ tenemos: $A = \mathbb{Q}[Z]$, $B = \mathbb{Q}[Z]/\mathfrak{p}_1 = \mathbb{Q}[Z]$ y $F = \mathbb{Q}(Z)$.

$$\mathbb{Q}[Y,Z] \xrightarrow{\quad\alpha\quad} \frac{\mathbb{Q}[Z]}{\mathfrak{p}_1}[Y] \xrightarrow{\quad\beta\quad} F[Y].$$

Tenemos que estudiar:
(i) si $\alpha(\mathfrak{p}_2)^e$ es primo en $\mathbb{Q}(Z)[Y]$ y
(ii) si $\alpha(\mathfrak{p}_2)$ es saturado en $\mathbb{Q}[Z][Y]$.

(i). Tenemos $\alpha(\mathfrak{p}_2)^e = (Y^5 - Z^4)\mathbb{Q}(Z)[Y]$. Ya que $Y^5 - Z^4$ es irreducible en $\mathbb{Q}(Z)[Y]$ entonces $\alpha(\mathfrak{p}_2)^e = (Y^5 - Z^4)\mathbb{Q}(Z)[Y]$ es un ideal primo. Para ver que $Y^5 - Z^4$ es irreducible podemos considerar el homomorfismo $\mathbb{Q}[Z][Y] \longrightarrow \mathbb{Q}[Y]$, definido por $Z \mapsto 2$, $Y \mapsto Y$; la imagen de $Y^5 - Z^4$ es $Y^5 - 16$ que es irreducible. Observar que el coeficiente líder de $h = Y^5 - Z^4 \in B[Y]$ es 1.

(ii). Estudiamos el ideal $(\alpha(\mathfrak{p}_2), 1-T)B[Y,T] \cap B[Y]$ para ver si coincide con $\alpha(\mathfrak{p}_2)$. Tenemos

$$\begin{aligned}
&(\alpha(\mathfrak{p}_2), 1-T)B[Y,T] \cap B[Y] = (Y^5 - Z^4, 1-T)\mathbb{Q}[Y,Z,T] \cap \mathbb{Q}[Y,Z],\\
&\alpha(\mathfrak{p}_2) = (Y^5 - Z^4)\mathbb{Q}[Y,Z].
\end{aligned}$$

Esta intersección se estudiar calculando las bases de Groebner respecto al orden lexicográfico con $T > Y > Z$. La base de Groebner reducida de $(Y^5 - Z^4, 1-T)\mathbb{Q}[Y,Z,T]$ es: $\{Y^5 - Z^4, 1-T\}$, y la de $(Y^5 - Z^4, 1-T)\mathbb{Q}[Y,Z,T] \cap \mathbb{Q}[Y,Z]$ es: $\{Y^5 - Z^4\}$. La base de Groebner reducida de $(Y^5 - Z^4)\mathbb{Q}[Y,Z]$ es: $\{Y^5 - Z^4\}$. Entonces ambos ideales son iguales y el ideal $\alpha(\mathfrak{p}_2)$ es saturado.

Como consecuencia el ideal $\mathfrak{p}_2 \subseteq \mathbb{Q}[Y,Z]$ es primo.

(3) Para $\mathfrak{p}_3 \subseteq \mathbb{Q}[X,Y,Z]$ tenemos

$$\begin{aligned}
&A = \mathbb{Q}[Y,Z],\\
&B = \mathbb{Q}[Y,Z]/(Y^5 - Z^4) = \mathbb{Q}[z] \oplus \mathbb{Q}[z]y \oplus \mathbb{Q}[z]y^2 \oplus \mathbb{Q}[z]y^3 \oplus \mathbb{Q}[z]y^4,\\
&F = \mathbb{Q}(z) \oplus \mathbb{Q}(z)y \oplus \mathbb{Q}(z)y^2 \oplus \mathbb{Q}(z)y^3 \oplus \mathbb{Q}(z)y^4.
\end{aligned}$$

Con la relación $y^5 = z^4$. (Aquí hemos representado a $\overline{Y}$ por y, y a $\overline{Z}$ por z.)

Al igual que antes tenemos que estudiar:
(i) si $\alpha(\mathfrak{p}_3)^e$ es primo en $F[X]$ y
(ii) si $\alpha(\mathfrak{p}_3)$ es saturado en $\mathbb{Q}[X,Y,Z]/(Y^5 - Z^4)$.

(i). El ideal $\alpha(\mathfrak{p}_3)^e$ está generado por los elementos

$$g_1 = Xz - y^2, \quad g_2 = Xy^3 - z^3, \quad g_3 = X^2y - z^2, \quad g_4 = X^3 - yz.$$

Como el ideal es principal basta calcular un generador. En este caso observamos que si llamamos $h' = X - y^2/z$ se tiene:

$$\begin{aligned}
&g_2 = h'y^3 + (y^5/z - z^3) = h'y^3,\\
&g_3 = h'(Xy + y^3/z) + (y^5/z^2 - z^2) = h'(Xy + y^3/z),\\
&g_4 = h'(X^2 + Xy^2/z + y^4/z^2) + (y^6/z^3 - yz) = h'(X^2 + Xy^2/z + y^4/z^2).
\end{aligned}$$

y se tiene: $\alpha(\mathfrak{p}_3)^e = (X - y^2/z) = (Xz - y^2)$. El coeficiente líder del generador $h = Xz - y^2 \in B[X]$ es z. El polinomio $h = Xz - y^2 \in F[X]$ es irreducible, ya que tiene grado uno.

(ii). Para estudiar la saturación de $\alpha(\mathfrak{p}_3)$ en $B[X]$, consideramos el ideal intersección $(\alpha(\mathfrak{p}_3), 1 - zT)B[X,T] \cap B[X]$ y lo comparamos con $\alpha(\mathfrak{p}_3)$. Pasamos a los anillos de polinomios con coeficientes en $\mathbb{Q}$ y calculamos las bases de Groebner reducidas respecto al orden lexicográfico con $T > X > Y > Z$.

$(\mathfrak{p}_3, 1 - ZT)\mathbb{Q}[T,X,Y,Z]$; la base de Groebner reducida es: $\{TY^2 - X, TZ - 1, X^3 - YZ, X^2Y - Z^2, XY^3 - Z^3, XZ - Y^2, Y^5 - Z^4\}$.

$(\mathfrak{p}_3, 1 - ZT)\mathbb{Q}[T,X,Y,Z] \cap \mathbb{Q}[X,Y,Z]$; la base de Groebner reducida es: $\{X^3 - YZ, X^2Y - Z^2, XY^3 - Z^3, XZ - Y^2, Y^5 - Z^4\}$.

Por lo tanto $(\mathfrak{p}_3, 1 - ZT)\mathbb{Q}[T,X,Y,Z] \cap \mathbb{Q}[X,Y,Z] = \mathfrak{p}_3$, luego $\alpha(\mathfrak{p}_3) = (\mathfrak{p}_3, 1 - zT)B[T,X,Y,Z] \cap \mathbb{Q}[X,Y,Z]$, y el ideal $\alpha(\mathfrak{p}_3)$ es saturado.

En consecuencia el ideal $\mathfrak{p}$ es un ideal primo de $\mathbb{Q}[X,Y,Z]$.

Ejercicio. 41.7.
Estudiar si el ideal $\mathfrak{p} = (XZ - Y^3, XY - Z^2) \subseteq \mathbb{Q}[X,Y,Z]$ *es primo.*

SOLUCIÓN. Con respecto al orden lexicográfico $X > Y > Z$ una base de Groebner reducida para $\mathfrak{p}$ es:

$$\{XY - Z^2, XZ - Y^3, Y^4 - Z^3\}.$$

$$\begin{aligned}
\mathfrak{p}_1 &= 0 \subseteq \mathbb{Q}[Z],\\
\mathfrak{p}_2 &= (Y^4 - Z^3) \subseteq \mathbb{Q}[Y,Z],\\
\mathfrak{p}_3 &= (XY - Z^2, XZ - Y^3, Y^4 - Z^3) \subseteq \mathbb{Q}[X,Y,Z].
\end{aligned}$$

(1) El ideal $\mathfrak{p}_1 \subseteq \mathbb{Q}[Z]$ es primo.

(2) El ideal $\mathfrak{p}_2 = (Y^4 - Z^3) \subseteq \mathbb{Q}[Y,Z]$ es primo.

(3) Para el ideal $\mathfrak{p}_3$ tenemos:

$$\begin{aligned}
A &= \mathbb{Q}[Y,Z],\\
B &= \mathbb{Q}[Y,Z]/(Y^4 - Z^3) = \mathbb{Q}[z] \oplus \mathbb{Q}[z]y \oplus \mathbb{Q}[z]y^2 \oplus \mathbb{Q}[z]y^3,\\
F &= \mathbb{Q}(z) \oplus \mathbb{Q}(z)y \oplus \mathbb{Q}(z)y^2 \oplus \mathbb{Q}(z)y^3.
\end{aligned}$$

Con la relación $y^4 = z^3$. El ideal $\alpha(\mathfrak{p}_3)$ está generado por los elementos:

$$g_1 = Xy - z^2, \quad g_2 = Xz - y^3.$$

El ideal $\alpha(\mathfrak{p}_3)^e$ está generado por un único elemento, que es:

$$h = Xy - z^2,$$

su coeficiente líder es y. Resulta que h es un elemento irreducible en $F[X]$, ya que es de grado uno. Entonces $\alpha(\mathfrak{p}_3)^e$ es un ideal primo de $F[X]$.

Estudiamos ahora la saturación de $\alpha(\mathfrak{p})$ en $B[X]$. Para esto comparamos $(\mathfrak{p}_3, 1 - YT)B[X, T] \cap A[X]$ y $\mathfrak{p}_3$.

Una base de Groebner reducida de $(\mathfrak{p}_3, 1 - YT)A[X, T] = (XY - Z^2, XZ - Y^3, Y^4 - Z^3, 1 - YT)$, respecto al orden lexicográfico con $T > X > Y > Z$, es:

$$\{TY - 1, TZ^2 - X, X^2 - Y^2Z, XY - Z^2, XZ - Y^3, Y^4 - Z^3\}.$$

Una base de Groebner reducida de $(\mathfrak{p}_3, 1 - YT)A[X, T] \cap A[X] = (XY - Z^2, XZ - Y^3, Y^4 - Z^3, 1 - YT) \cap \mathbb{Q}[X, Y, Z]$, respecto al mismo orden, es:

$$\{X^2 - Y^2Z, XY - Z^2, XZ - Y^3, Y^4 - Z^3\},$$

y como no coincide con la base de Groebner reducida de $\mathfrak{p}_3$, resulta que $\alpha(\mathfrak{p}_3)$ no es saturado, y en consecuencia $\mathfrak{p} = \mathfrak{p}_3$ no es un ideal primo.

Observa que como la saturación de $\alpha(\mathfrak{p})$ es el ideal $(X^2 - Y^2Z, XY - Z^2, XZ - Y^3, Y^4 - Z^3)$ y como ésta no coincide con $\mathfrak{p}$, alguno de sus generadores no está en $\mathfrak{p}$, en este caso $X^2 - Y^2Z$, resulta que, como $b = y$, el producto $Y(X^2 - Y^2Z) \in \mathfrak{p}$, pero ninguno de estos factores pertenece a $\mathfrak{p}$, lo cual muestra explícitamente dos elementos que prueban que $\mathfrak{p}$ no es primo.

$$Y(X^2 - Y^2Z) = X^2Y - Y^3Z = X(XY - Z^2) + Z(XZ - Y^3).$$

□

Ejercicio. 41.8.
Sea $\mathfrak{a} = (XZ - Y^3, XY^2 - Z^2) \subseteq \mathbb{Q}[X, Y, Z]$. Vamos a ver que $\mathfrak{a}$ no es un ideal primo determinando elementos $a, b \in \mathbb{Q}[X, Y, Z]$ tales que $a, b \in \mathbb{Q}[X, Y, Z]$ con $ab \in \mathfrak{a}$ y $a, b \notin \mathfrak{a}$.

SOLUCIÓN. Una base de Groebner de $\mathfrak{a}$ con respecto al orden lexicográfico $X > Y > Z$ es:

```
> GroebnerBasis[{X Z - Y^3, X Y^2 - Z^2}, {X, Y, Z}]
```

$$\{XY^2 - Z^2, XZ - Y^3, Y^5 - Z^3\},$$

Por lo tanto $\mathfrak{a} \cap \mathbb{Q}[Z] = \{0\}$ es un ideal primo.
También $\mathfrak{a} \cap \mathbb{Q}[Y, Z] = (Y^5 - Z^2)$ es un ideal primo.

Tenemos los homomorfismos

$$\mathbb{Q}[X,Y,Z] \xrightarrow{\alpha} \frac{\mathbb{Q}[Y,Z]}{\mathfrak{a}\cap\mathbb{Q}[Y,Z]}[X] = \frac{\mathbb{Q}[Y,Z]}{(Y^5-Z^2)}[X] \xrightarrow{\beta} \mathbb{Q}(y,z)[X].$$

Estudiamos la saturación de $\alpha(\mathfrak{a})$. Tenemos:

$$\alpha(\mathfrak{a})^e = (Xz-y^3, Xy^2-z^2)\mathbb{Q}(y,z)[X].$$

Como

$$Xz-y^3 = \frac{1}{z^2}(Xz^3-y^3z^2) = \frac{1}{z^2}(Xy^5-y^3z^2) = \frac{y^3}{z^2}(Xy^2-z^2) \in (Xy^2-z^2)\mathbb{Q}(y,z)[X],$$

entonces

$$\alpha(\mathfrak{a})^e = (Xy^2-z^2)\mathbb{Q}(y,z)[X] = (Xz-y^3)\mathbb{Q}(y,z)[X],$$

es un ideal primo. El coeficiente líder de Xy^2-z^2 es z^2, y se tiene $z\notin\alpha(\mathfrak{a})$. Calculamos $(\alpha(\mathfrak{a}), 1-zT)\mathbb{Q}(y,z)[X]$, y para esto nos trasladamos a $\mathbb{Q}[X,Y,Z]$ con el orden lexicográfico $T>X>Y>Z$. Se tiene:

$$(\mathfrak{a}, 1-ZT) = (XY^2-Z^2, XZ-Y^3, Y^5-Z^3, ZT-1).$$

Una base de Groebner es:

```
> GroebnerBasis[{XY^2-Z^2,XZ-Y^3,Y^5-Z^3,ZT-1},{T,X,Y,Z}]
```

$$\{TY^3-X, TZ-1, X^2-YZ, XY^2-Z^2, XZ-Y^3, Y^5-Z^3\}.$$

Y se verifica:

$$(\mathfrak{a}, 1-ZT)\cap\mathbb{Q}[X,T,Z] = (X^2-YZ, XY^2-Z^2, XZ-Y^3, Y^5-Z^3),$$

que contiene propiamente a $\mathfrak{a}$, ya que $X^2-YZ\notin\mathfrak{a}$.
Podemos ahora dar los elementos que andamos buscando. Tomamos $a=Z$ y $b=X^2-YZ$. Se verifica

$$Z(X^2-YZ) \equiv X^2Z-YZ^2 \equiv XY^3-YZ^2 \equiv Z^2Y-YZ^2 \equiv 0 \pmod{\mathfrak{a}}.$$

□

Ejercicio. 41.9.
Vamos a ver que el ideal $\mathfrak{p} = (XZ-Y^3, XY^2-Z^2, X^2-YZ) \subseteq \mathbb{Q}[X,Y,Z]$ *es un ideal primo.*

SOLUCIÓN. Calculamos una base de Groebner del ideal $\mathfrak{p} = (XZ-Y^3, XY^2-Z^2, X^2-YZ)$ para el orden lexicográfico con $X>Y>Z$.

```
> GroebnerBasis[{X Z-Y^3, X Y^2-Z^2, X^2-Y Z}, {X, Y, Z}]
```

$$\{X^2-YZ, XY^2-Z^2, XZ-Y^3, Y^5-Z^3\}$$

Calculamos las eliminaciones:
$\mathfrak{p}\cap\mathbb{Q}[Z]=\{0\}$ es un ideal primo.
$\mathfrak{p}\cap\mathbb{Q}[Y,Z]=(Y^5-Z^3)$ es un ideal primo.
Consideramos los homomorfismos

$$\mathbb{Q}[X,Y,Z]\stackrel{\alpha}{\longrightarrow}\frac{\mathbb{Q}[Y,Z]}{(Y^5-Z^3)}[X]\stackrel{\beta}{\longrightarrow}\mathbb{Q}(y,z)[X].$$

Calculamos $\alpha(\mathfrak{p})^e$:

$$\alpha(\mathfrak{p})^e=(Xz-y^3, Xy^2-z^2, X^2-yz)\mathbb{Q}(y,z)[X]=(Xz-y^3)\mathbb{Q}(y,z)[X].$$

El término líder es z y $z\notin\alpha(\mathfrak{p})$.
Calculamos el contraído $\alpha(\mathfrak{p})^{ec}$; para esto pasamos a $\mathbb{Q}[T,X,Y,Z]$ y calculamos el ideal $(\mathfrak{p},1-ZT)$:

$$(\mathfrak{p},1-ZT)=(XZ-Y^3, XY^2-Z^2, X^2-YZ, 1-ZT)$$

Una base de Groebner para el orden lexicográfico con $T>X>Y>Z$ es:

```
> GroebnerBasis[{XZ-Y^3,XY^2-Z^2,X^2-YZ,1-ZT},{T,X,Y,Z}]
```

$$\{TY^3-X, TZ-1, X^2-YZ, XY^2-Z^2, XZ-Y^3, Y^5-Z^3\}$$

El contraído se obtiene a partir de $(\mathfrak{p},1-ZT)\cap\mathbb{Q}[X,Y,Z]$, que es:

$$(X^2-YZ, XY^2-Z^2, XZ-Y^3, Y^5-Z^3),$$

que coincide con $\mathfrak{p}$, luego $\mathfrak{p}$ es primo. □

Ejercicio. 41.10.
Demuestra que el ideal $\mathfrak{p}=(XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5)\subseteq\mathbb{Q}[X,Y,Z,W]$ *es un ideal primo.*

SOLUCIÓN.

```
>GroebnerBasis[{XZ^2-W^3,XW^2-Y^4,Y^4Z^2-W^5},{X,Y,Z,W}]
```

Base de Groebner:

$$\{XZ^2 - W^3, XW^2 - Y^4, Y^4Z^2 - W^5\}.$$

$\mathfrak{p} \cap \mathbb{Q}[W] = \{0\}$.
$\mathfrak{p} \cap \mathbb{Q}[Z, W] = \{0\}$.
$\mathfrak{p} \cap \mathbb{Q}[Y, Z, W] = (Y^4Z^2 - W^5)$ es un ideal primo.

$$\mathbb{Q}[X, Y, Z, W] \xrightarrow{\alpha} \frac{\mathbb{Q}[Y, Z, W]}{(Y^4Z^2 - W^5)}[X] \xrightarrow{\beta} \mathbb{Q}(y, z, w)[X].$$

Extendido $\alpha(\mathfrak{p})^e = (Xz^2 - w^3)Q(y, z, w)[X]$, ya que

$$Xz^2 - w^3 = \frac{w^3}{y^4}(Xw^2 - y^4).$$

El coeficiente líder es z^2. Para calcular el contraído pasamos a $\mathbb{Q}[X, Y, Z, W]$:

$$(\mathfrak{p}, 1 - Z^2T) = (XZ^2 - W^3, XW^2 - Y^4, Y^4Z^2 - W^5, 1 - ZT).$$

Una base de Groebner para el orden lexicográfico con $T > X > Y > Z > W$ es:

```
> GroebnerBasis[{XZ^2-W^3,X W^2-Y^4,Y^4Z^2-W^5,1-ZT},{T,X,Y,Z,W}]
```

$$\{TY^8 - WX^3Z, TY^4W - X^2Z, TZ - 1, TW^3 - XZ, Y^4Z^2 - W^5, XZ^2 - W^3, XW^2 - Y^4\}$$

Y el contraído es la imagen de:

$$(Y^4Z^2 - W^5, XZ^2 - W^3, XW^2 - Y^4) = \mathfrak{p}.$$

Luego el ideal $\mathfrak{p}$ es primo. □

Ejercicio. 41.11.
Demuestra que el ideal $\mathfrak{a} = (XY - W^3, Y^2 - ZW) \subseteq \mathbb{Q}[X, Y, Z, W]$ no es un ideal primo.

SOLUCIÓN. $\mathfrak{p} = (XY - W^3, Y^2 - ZW)$ tiene base de Groebner para el orden lexicográfico con $X > Y > Z > W$

```
> GroebnerBasis[{X Y - W^3, Y^2 - Z W}, {X, Y, Z, W}]
```

$$\{XY - W^3, XZW - YW^3, Y^2 - WZ\}$$

Los ideales eliminación son:
$\mathfrak{p} \cap \mathbb{Q}[W] = \{0\}$
$\mathfrak{p} \cap \mathbb{Q}[Z, W] = \{0\}$

$\mathfrak{p} \cap \mathbb{Q}[Y, Z, W] = (Y^2 - WZ)$ que es primo.

$$\mathbb{Q}[X, Y, Z, W] \xrightarrow{\alpha} \frac{\mathbb{Q}[Y, Z, W]}{(Y^2 - WZ)} \xrightarrow{\beta} \mathbb{Q}(y, z, w)[X].$$

Extendido

$$\alpha(\mathfrak{p})^e = (Xy - w^3)Q(y, z, w)[X],$$

El coeficiente líder es $y \notin \alpha(\mathfrak{a})$. Para calcular el contraido pasamos a $\mathbb{Q}[X, Y, Z, W]$; calculamos el ideal $(\mathfrak{p}, 1 - YT) = (XY - W^3, Y^2 - ZW, 1 - YT)$. una base de Groebner es:

```
> GroebnerBasis[{X Y - W^3, Y^2 - Z W, 1 - Y T}, {T, X, Y, Z, W}]
```

$$\{TY - 1, TWZ - Y, TW^3 - X, XY - W^3, XZ - W^2Y, Y^2 - WZ\}$$

La intersección con $\mathbb{Q}[X, Y, Z, W]$ es:

$$(XY - W^3, XZ - W^2Y, Y^2 - WZ).$$

Este ideal contiene a $\mathfrak{p}$, pero no está contenido en $\mathfrak{p}$, ya que $XZ - W^2Y \notin \mathfrak{p}$. En efecto,

```
> PolynomialReduce[X Z-W^2 Y,{Y^2-W Z,W X Z-W^3Y,X Y-W^3},{X,Y,Z,W}]

El resultado es: {{0,0,0},X Z-W^2 Y}
```

Esto significa que $Y(XZ - W^2Y) = Z(XY - W^3) - W^2(Y^2 - WZ) \in \mathfrak{p}$. □

Cálculo de la dimensión

Dado un ideal primo $\mathfrak{p} \in K[X_1, \ldots, X_n]$, se define:

$$\begin{aligned} &\mathfrak{p}_0 = 0 \\ &\mathfrak{p}_i = \mathfrak{p} \cap K[X_1, \ldots, X_i] \quad \text{si } i = 1, \ldots, n. \end{aligned}$$

Para cada índice i existe un homomorfismo

$$\begin{array}{ccc} \frac{K[X_1,\ldots,X_{i-1}]}{\mathfrak{p}_{i-1}} & \xrightarrow{\quad\alpha\quad} & \frac{K[X_1,\ldots,X_i]}{\mathfrak{p}_i} \\ \| & & \\ \frac{K[X_1,\ldots,X_{i-1}]}{\mathfrak{p}_i \cap K[X_1,\ldots,X_{i-1}]} & & \end{array}$$

y por tanto $A := \frac{K[X_1,\ldots,X_{i-1}]}{\mathfrak{p}_{i-1}}$ es una subalgebra de $B := \frac{K[X_1,\ldots,X_i]}{\mathfrak{p}_i}$, y B se genera sobre A por un elemento, la clase de X_i. En consecuencia, por el lema de normalización tenemos $\dim(A) \leq \dim(B) \leq \dim(a) + 1$. Supongamos que $\mathfrak{p}_{i-1}^e = \mathfrak{p}_i$, entones en B la clase de X_i es algebraicamente independiente sobre A y se tiene $\dim(B) = \dim(A) + 1$.

Supongamos que $\mathfrak{p}_{i-1}^e \neq \mathfrak{p}_i$, entonces $\dim(A) = \dim(B)$.
Podemos entonces determinar la dimensión de $K[X_1,\ldots,X_n]/\mathfrak{p}$ considerando las dimensiones de los cocientes $K[X_1,\ldots,X_i]/\mathfrak{p}_i$. A´si podemos enunciar

$$\dim(K[X_1,\ldots,X_n]/\mathfrak{p}) = \mathrm{Card}(\{i \mid \ i=1,\ldots,n,\ \mathfrak{p}_{i-1}^e = \mathfrak{p}_i\}).$$

Para un cálculo algorítmico basta considerar una base de Groebner reducida $\mathbb{G}$ de $\mathfrak{p}$ respecto al orden lexicográfico $X_n > X_{n-1} > \cdots > X_1$. Entonces la bases del ideal $\mathfrak{p}_i$ es $\mathbb{G}_i = \mathbb{G} \cap K[X_1,\ldots,X_i]$, y se tiene $\mathfrak{p}_{i-1}^e = \mathfrak{p}_i$ si y solo si $\mathbb{G}_{i-1} = \mathbb{G}_i$. Como consecuencia tenemos un modo de calcular la dimensión del cociente $K[X_1,\ldots,X_n]/\mathfrak{p}$.

Ejercicio. 41.12.
Determina la dimensión del anillo $\mathbb{Q}[X,Y,Z,W]/(XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5)$.

SOLUCIÓN. Basta determinar una base de Groebner del ideal $(XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5)$. Ésta es:

$$\{XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W5\}$$

Observa que hemos utilizado el orden lexicográfico con $X > Y > Z > W$, entones consideramos la lista de ideales

$$\begin{array}{l}
\mathfrak{p} = (XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5) \cap \mathbb{Q}[X,Y,Z,W]; \\
\mathfrak{p}_3 = (XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5) \cap \mathbb{Q}[Y,Z,W]; \\
\mathfrak{p}_2 = (XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5) \cap \mathbb{Q}[Z,W]; \\
\mathfrak{p}_1 = (XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5) \cap \mathbb{Q}[W]; \\
\mathfrak{p}_0 = 0
\end{array}$$

y las álgebras correspondientes. Las bases de Groebner son:

$$\begin{array}{ll}
\mathbb{G} = \{XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W5\} & = \\
\mathbb{G}_3 = \{Y^4Z^2-W5\} & = \\
\mathbb{G}_2 = \varnothing & +1 \\
\mathbb{G}_1 = \varnothing & +1 \\
\mathbb{G}_0 = \varnothing &
\end{array}$$

La dimensión de $\mathbb{Q}[X,Y,Z,W]/(XZ^2-W^3, XW^2-Y^4, Y^4Z^2-W^5)$ es igual a 2. □

42. Módulos de fracciones

Producto tensor

Sea A un anillo (conmutativo). Recordemos la definición de producto tensor de dos A–módulos.
Sean M_1 y M_2 dos A–módulos, definimos un nuevo A–módulo al que representaremos por $M_1 \otimes_A M_2$ mediante el siguiente proceso:
Tomamos el grupo abeliano libre G sobre $M_1 \times M_2$ y el subgrupo S generado por los elementos

$$\begin{array}{ll} (a, b_1 + b_2) - (a, b_1) - (a, b_2); & \forall a \in M_1; b_1, b_2 \in M_2; \\ (a_1 + a_2, b) - (a_1, b) - (a_2, b); & \forall a_1, a_2 \in M_1; b \in M_2; \\ (a, rb) - (ra, b); & \forall a \in M_1; b \in M_2; r \in A. \end{array}$$

De esta forma el cociente G/S es un grupo abeliano al que llamaremos $M_1 \otimes_A M_2$. Los elementos de $M_1 \otimes_A M_2$ son combinaciones lineales (en A) de clases de pares (x, y), con $x \in M_1$ e $y \in M_2$, a las que vamos a representar por $x \otimes y$. De esta forma cada elemento de $M_1 \otimes_A M_2$ se escribe en la forma:

$$\sum_{i=1}^{n} a_i x_i \otimes y_i, \qquad a_i \in A; x_i \in M_1; \quad y_i \in M_2.$$

Existe una acción de A sobre $M_1 \otimes_A M_2$ mediante:

$$a(x \otimes y) = (ax) \otimes y = x \otimes (ay)$$

Se tienen homomorfismos de A–módulos de M_i en $M_1 \otimes_A M_2$ definidos:

$$M_1 \to M_1 \otimes_A M_2; \quad x \mapsto x \otimes y, \text{ para } y \text{ fijo}$$

$$M_2 \to M_1 \otimes_A M_2; \quad y \mapsto x \otimes y, \text{ para } x \text{ fijo}$$

Una aplicación $\varphi : M_1 \times M_2 \to M$ se llama **bilineal** si verifica las propiedades siguientes:

$$\begin{array}{llll} \varphi(a, b_1 + b_2) = \varphi(a, b_1) + \varphi(a, b_2); & \forall a \in M_1; & \forall b_1, b_2 \in M_2. & \\ \varphi(a_1 + a_2, b) = \varphi(a_1, b) + \varphi(a_2, b); & \forall a_1, a_2 \in M_1; & \forall b \in M_2. & \\ \varphi(a, rb) = \varphi(ra, b); & \forall a \in M_1; & \forall b \in M_2; & \forall r \in A. \end{array}$$

Es claro que la aplicación $t : M_1 \times M_2 \to M_1 \otimes_A M_2$ definida por $t(x, y) = x \otimes y$ es bilineal.

Teorema. 42.1. (Propiedad universal del producto tensor.)
Sean M_1, M_2 y M tres A–módulos y $f : M_1 \times M_2 \to M$ una aplicación bilineal, existe un único homomorfismo de A–módulos $f' : M_1 \otimes_A M_2 \to M$ tal que $f = f' \circ t$.

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\ t\ } & M_1 \otimes_A M_2 \\ & {\scriptstyle f} \searrow \quad \swarrow {\scriptstyle f'} & \\ & M & \end{array}$$

Teorema. 42.2.
Para cada A–módulo M tenemos definido un funtor $M \otimes_A - : A-\textbf{Mod} \to A-\textbf{Mod}$, que es adjunto a la derecha del funtor $\operatorname{Hom}_A(M,-) : A-\textbf{Mod} \to A-\textbf{Mod}$, y por lo tanto es exacto a la derecha y conserva colímites.

$$\begin{array}{c} A-\textbf{Mod} \\ {\scriptstyle M\otimes_A -}\downarrow \uparrow {\scriptstyle \operatorname{Hom}_A(M,-)} \\ A-\textbf{Mod} \end{array}$$

DEMOSTRACIÓN. Consideramos la aplicación:

$$\operatorname{Hom}_A(M \otimes_A X, Y) \stackrel{\omega_{X,Y}}{\longrightarrow} \operatorname{Hom}_A(X, \operatorname{Hom}_A(M,Y)),$$

definida $\omega_{X,Y}(f)(x)(m) = f(m \otimes x)$.
Se tiene que $\omega_{X,Y}$ es una biyección natural en X e Y. □

Si el funtor $M \otimes_A -$ es un funtor exacto, entonces M se llama un A–módulo **plano**.

Localización

Sea A un anillo conmutativo, Σ un subconjunto multiplicativo y M un A–módulo. Definimos $\Sigma^{-1}M$ el **módulo de fracciones** de M respecto a Σ como el conjunto $M \times \Sigma$ bajo la relación de equivalencia

$$(m_1, s_1) \equiv (m_2, s_2) \text{ si existe } t \in \Sigma \text{ tal que } (m_1 s_2 - m_2 s_1)t = 0$$

La clase $\overline{(m,s)}$ se representa por m/s.
Las operaciones en $\Sigma^{-1}M$ están definidas de forma que:
(1) $\Sigma^{-1}M$ es un grupo abeliano: $m_1/s_1 + m_2/s_2 = (m_1 s_2 + m_2 s_1)/(s_1 s_2)$;
(2) $\Sigma^{-1}M$ es un A–módulo: $r(m/s) = (rm)/s$;
(3) $\Sigma^{-1}M$ es un $\Sigma^{-1}A$–módulo: $(r/s_1)(m/s_2) = (rm)/(s_1 s_2)$.

Para cada A–módulo M existe un homomorfismo de A–módulos $\lambda_M = \lambda_{\Sigma,M} : M \to \Sigma^{-1}M$.

Lema. 42.3.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo:
(1) Si M es un A–módulo, entonces $\Sigma^{-1}M$ es un A–módulo via el homomorfismo $\lambda : A \to \Sigma^{-1}A$;
(2) Si N es un $\Sigma^{-1}A$–módulo y consideramos la estructura de A–módulo vía $\lambda_A : A \to \Sigma^{-1}A$, entonces $N \cong \Sigma^{-1}N$.

Proposición. 42.4. (Propiedad universal del módulo de fracciones.)
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo. Sea $f : M \to N$ un homomorfismo de A–módulos, siendo N un $\Sigma^{-1}A$–módulo, existe un único homomorfismo de $\Sigma^{-1}A$–módulos $f' : \Sigma^{-1}M \to N$ tal que $f = \lambda_M \circ f'$.

$$\begin{array}{ccc} M & \xrightarrow{\lambda_M} & \Sigma^{-1}M \\ & {\scriptstyle f}\searrow \quad \swarrow{\scriptstyle f'} & \\ & N & \end{array}$$

Corolario. 42.5.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo. Sean $f : M \to N$ un homomorfismo de A–módulos; entonces existe un único homomorfismo $\Sigma^{-1}f$ de $\Sigma^{-1}A$–módulos tal que $f \circ \lambda_N = \lambda_M \circ \Sigma^{-1}f$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle \lambda_M}\downarrow & & \downarrow{\scriptstyle \lambda_N} \\ \Sigma^{-1}M & \dashrightarrow_{\Sigma^{-1}f} & \Sigma^{-1}N \end{array}$$

Corolario. 42.6.
Sea A un anillo, $\Sigma \subseteq A$ un subconjunto. Se verifica:
(1) Si $f : M \longrightarrow M'$ y $g : M' \longrightarrow M$” son homomorfismos de A–módulos, $\Sigma^{-1}(g \circ f) = \Sigma^{-1}g \circ \Sigma^{-1}f$.
(2) Para cada A–módulo M se tiene $\Sigma^{-1}\,\mathrm{id}_M = \mathrm{id}_{\Sigma^{-1}M}$.

Tenemos entonces una situación de adjunción

$$\begin{array}{c} A\text{–}\textbf{Mod} \\ {\scriptstyle \Sigma^{-1}}\downarrow\uparrow{\scriptstyle \mathcal{U}} \\ \Sigma^{-1}A\text{–}\textbf{Mod} \end{array}$$

Proposición. 42.7.
Sea A un anillo conmutativo y Σ un subconjunto multiplicativo. Si $0 \to M' \to M \to M'' \to 0$ es una sucesión exacta corta de A–módulos, entonces

$$0 \to \Sigma^{-1}M' \to \Sigma^{-1}M \to \Sigma^{-1}M'' \to 0$$

es una sucesión exacta corta de $\Sigma^{-1}A$–módulos.

Corolario. 42.8.
Sea A un anillo, $\Sigma \subseteq A$ un subconjunto multiplicativo y $M_1, M_2 \subseteq M$ submódulos, se verifica:

(1) $\Sigma^{-1}M_i$ es un submódulo de $\Sigma^{-1}M$.
(2) $\Sigma^{-1}(M_1 + M_2) = \Sigma^{-1}M_1 + \Sigma^{-1}M_2$.
(3) $\Sigma^{-1}(M_1 \cap M_2) = \Sigma^{-1}M_1 \cap \Sigma^{-1}M_2$.
(4) $\Sigma^{-1}M/\Sigma^{-1}M_1 \cong \Sigma^{-1}(M/M_1)$.

Corolario. 42.9.
Sea A un anillo, $\Sigma \subseteq A$ un subconjunto multiplicativo y M_1, M_2 dos A–módulos, se verifica:

$$\Sigma^{-1}(M_1 \oplus M_2) \cong \Sigma^{-1}M_1 \oplus \Sigma^{-1}M_2.$$

Teorema. 42.10.
Sea A un anillo y Σ un subconjunto multiplicativo. Para cada A–módulo M existe un isomorfismo natural $\sigma : \Sigma^{-1}A \otimes_A M \cong \Sigma^{-1}M$ definido por: $\sigma(a/s \otimes m) = am/s$.

Consecuencia de los anteriores resultados tenemos:

Corolario. 42.11.
En la situación anterior $\Sigma^{-1}A$ es un A–módulo plano.

En este caso se tiene también una situación de adjunción

$$\begin{array}{c} A-\textbf{\textit{Mod}} \\ \Sigma^{-1}A\otimes_A - \Big\downarrow \Big\uparrow Hom_{\Sigma^{-1}A}(\Sigma^{-1}A,-) \\ \Sigma^{-1}A-\textbf{\textit{Mod}} \end{array}$$

Observar que hemos encontrado dos adjuntos a la derecha del funtor $\Sigma^{-1}(-) = \Sigma^{-1}A \otimes_A -$.

Lema. 42.12.
Sea A un anillo y Σ un subconjunto multiplicativo; si M y N son A–módulos, entonces existe un isomorfismo de $\Sigma^{-1}A$–módulos

$$\Sigma^{-1}M \otimes_{\Sigma^{-1}A} \Sigma^{-1}N \cong \Sigma^{-1}(M \otimes_A N).$$

DEMOSTRACIÓN. Tenemos una sucesión de isomorfismos naturales:

$$\begin{aligned} \Sigma^{-1}M \otimes_{\Sigma^{-1}A} \Sigma^{-1}N &\cong M \otimes_A \Sigma^{-1}A \otimes_{\Sigma^{-1}A} \Sigma^{-1}N \cong M \otimes_A \Sigma^{-1}N \\ &\cong M \otimes_A \Sigma^{-1}A \otimes_A \Sigma^{-1}N \qquad \cong \Sigma^{-1}A \otimes_A (M \otimes_A N) \\ &\cong \Sigma^{-1}(M \otimes_A N). \end{aligned}$$

□

La propiedad análoga para el funtor Hom_A sería:

$$\operatorname{Hom}_{\Sigma^{-1}A}(\Sigma^{-1}M, \Sigma^{-1}N) \cong \Sigma^{-1}\operatorname{Hom}_A(M,N).$$

que en general no se verifica. En el caso en que M es finitamente presentado (un A–módulo M es **finitamente presentado** si existe una presentación libre $A^m \to A^n \to M \to 0$ con $m,n \in \mathbb{N}$) tenemos:

Lema. 42.13.
Sea A un anillo conmutativo y M, N dos A–módulos tales que M es finitamente presentado, entonces para cada subconjunto multiplicativo Σ se tiene un isomorfismo natural

$$\operatorname{Hom}_{\Sigma^{-1}A}(\Sigma^{-1}M, \Sigma^{-1}N) \cong \Sigma^{-1}\operatorname{Hom}_A(M,N).$$

DEMOSTRACIÓN. Consideramos una presentación libre de M, por ejemplo $A^m \longrightarrow A^n \longrightarrow M \longrightarrow 0$. Aplicando los funtores $\operatorname{Hom}_A(-,N)$ y Σ^{-1} en distinto orden tenemos una diagrama conmutativo con

filas exactas:

$$\begin{array}{ccccccc}
0 \longrightarrow & \Sigma^{-1}\operatorname{Hom}_A(M,N) & \longrightarrow & \Sigma^{-1}\operatorname{Hom}_A(A^n,N) & \longrightarrow & \Sigma^{-1}\operatorname{Hom}_A(A^m,N) \\
& \downarrow & & \| & & \| \\
& & & \Sigma^{-1}N^n & & \Sigma^{-1}N^m \\
& & & \| & & \| \\
0 \longrightarrow & \operatorname{Hom}_{\Sigma^{-1}A}(\Sigma^{-1}M,\Sigma^{-1}N) & \longrightarrow & \operatorname{Hom}_{\Sigma^{-1}A}(\Sigma^{-1}A^n,\Sigma^{-1}N) & \longrightarrow & \operatorname{Hom}_{\Sigma^{-1}A}(\Sigma^{-1}A^m,\Sigma^{-1}N)
\end{array}$$

Por la propiedad universal del núcleo tenemos el resultado □

Lema. 42.14.
Sea A un anillo conmutativo, Σ un subconjunto multiplicativo y M un A–módulo finitamente generado. Entonces

$$\Sigma^{-1}\operatorname{Ann}_A(M) = \operatorname{Ann}_{\Sigma^{-1}A}(\Sigma^{-1}M).$$

DEMOSTRACIÓN. Supongamos que el resultado es cierto para dos módulos M_1 y M_2, entonces se tiene

$$\begin{aligned}
\Sigma^{-1}(0:M_1+M_2)_A &= \Sigma^{-1}((0:M_1)_A \cap (0:M_2))_A \\
&= \Sigma^{-1}(0:M_1)_A \cap \Sigma^{-1}(0:M_2)_A \\
&= (0:\Sigma^{-1}M_1)_{\Sigma^{-1}A} \cap (0:\Sigma^{-1}M_2)_{\Sigma^{-1}A} \\
&= (0:(\Sigma^{-1}M_1+\Sigma^{-1}M_2))_{\Sigma^{-1}A} \\
&= (0:\Sigma^{-1}(M_1+M_2))_{\Sigma^{-1}A}.
\end{aligned}$$

Basta entonces probar el resultado para módulos cíclicos. Sea $M = Aa \cong A/\mathfrak{a}$, entonces

$$\Sigma^{-1}(A/\mathfrak{a}) = \Sigma^{-1}A/\Sigma^{-1}\mathfrak{a},$$

y se tiene

$$\Sigma^{-1}(0:A/\mathfrak{a})_A = \Sigma^{1}\mathfrak{a} = (0:\Sigma^{-1}A)_{\Sigma^{-1}A}.$$

□

Corolario. 42.15.
Sea A un anillo conmutativo, Σ un subconjunto multiplicativo y M un A–módulo. Entonces para cada par de submódulos $N,H \subseteq M$, H finitamente generado, se verifica:

$$\Sigma^{-1}(N:H)_A = (\Sigma^{-1}N:\Sigma^{-1}H)_{\Sigma^{-1}A}.$$

DEMOSTRACIÓN. Basta tener en cuenta que $(N:H)_A = (0:(N+H)/N)_A$ y aplicar el Lema (42.14.). □

Propiedades locales

Dado un anillo A, un A–módulo M y un ideal primo $\mathfrak{p}$ consideramos el subconjunto multiplicativo $\Sigma = A \setminus \mathfrak{p}$. El anillo de fracciones $\Sigma^{-1}A$ se representa por $A_\mathfrak{p}$, y el módulo de fracciones $\Sigma^{-1}M$ se representa por $M_\mathfrak{p}$.

Una propiedad de anillos ó de módulos $\mathcal{P}$ es una **propiedad local** si A ó M la tienen si y solo si $A_\mathfrak{p}$ ó $M_\mathfrak{p}$ la tienen para cada ideal primo $\mathfrak{p}$. Ya hemos comprobado, ver Proposición (40.23.), que la propiedad de ser un dominio normal es una propiedad local.

Lema. 42.16.
Sea M un A–módulo. Son equivalentes los siguientes enunciados:

(a) $M = 0$;
(b) $M_\mathfrak{p} = 0$ *para cada ideal primo* $\mathfrak{p}$;
(c) $M_\mathfrak{m} = 0$ *para cada ideal maximal* $\mathfrak{m}$.

Como consecuencia tenemos el siguiente resultado sobre representación de módulos:

Proposición. 42.17.
Sea A un anillo conmutativo y M un A–módulo, entonces la aplicación canónica

$$M \longrightarrow \prod\{M_\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Spec}(R)\}$$

es inyectiva.

Corolario. 42.18.
Sea A un anillo conmutativo y $f : M \to N$ un homomorfismo de A–módulos. Son equivalentes los siguientes enunciados:

(a) f *es inyectivo (resp. sobreyectivo);*
(b) $f_\mathfrak{p} : M_\mathfrak{p} \to N_\mathfrak{p}$ *es inyectivo (resp. sobreyectivo) para cada ideal primo* $\mathfrak{p}$ *de* A;
(c) $f_\mathfrak{m} : M_\mathfrak{m} \to N_\mathfrak{m}$ *es inyectivo (resp. sobreyectivo) para cada ideal maximal* $\mathfrak{m}$ *de* A.

Corolario. 42.19.
Sea A un anillo conmutativo y N un submódulo de un A–módulo M. Para cada $x \in M$ son equivalentes los siguientes enunciados:

(a) $x \in N$;
(b) $x/1 \in N_{\mathfrak{p}}$ *para cada ideal primo* $\mathfrak{p}$ *de* A;
(c) $x/1 \in N_{\mathfrak{m}}$ *para cada ideal maximal* $\mathfrak{m}$ *de* A.

Proposición. 42.20.
Sea A *un anillo conmutativo y* M *un* A*–módulo. Son equivalentes los siguientes enunciados:*

(a) M *es un* A*–módulo plano;*
(b) $M_{\mathfrak{p}}$ *es un* A*–módulo plano para cada ideal primo* $\mathfrak{p}$ *de* A;
(c) $M_{\mathfrak{m}}$ *es un* A*–módulo plano para cada ideal maximal* $\mathfrak{m}$ *de* A.

Submódulos de torsión

Si D es un dominio de integridad el localizado $D_{(0)}$ es K, el cuerpo de fracciones de D. Para cada D–módulo M la localización $M_{(0)}$ es un espacio vectorial sobre K. El núcleo del homomorfismo $\lambda_M : M \longrightarrow M_{(0)}$ el justamente el **submódulo de torsión** de M, esto es,

$$\mathrm{Ker}(\lambda_M) = T(M) = \{m \in M \mid \text{ existe } 0 \neq d \in D \text{ tal que } dm = 0\}.$$

Dado un dominio D, para cada elemento $0 \neq a \in D$, el núcleo del homomorfismo $\lambda_M : M \longrightarrow M_a$ son los **elementos de a–torsión**.

$$\mathrm{Ker}(\lambda_M) = T_a(M) = \{m \in M \mid a^n m = 0, \text{ para algún } n \in \mathbb{N}\}.$$

Espectro de un anillo

Dado un anillo A, el conjunto de los ideales primos de A lo representamos por $\mathrm{Spec}(A)$, y lo llamamos el **espectro** de A.
En el espectro de un anillo A definimos una topología tomando como conjuntos cerrados los conjuntos

$$\mathcal{V}(\mathfrak{a}) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq \mathfrak{a}\},$$

donde $\mathfrak{a}$ varía entre los ideales de A, y para cada elemento $a \in A$ definimos $\mathcal{V}(a) = \mathcal{V}(Aa)$.

Lema. 42.21.
Los conjuntos $\mathcal{V}(\mathfrak{a})$ *son los conjuntos cerrados para una topología en* $\mathrm{Spec}(A)$.

Los conjuntos abiertos son los complementos de los cerrados, por lo tanto son de la forma:

$$X(\mathfrak{a}) = \operatorname{Spec}(A) \setminus \mathcal{V}(\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(a) \mid \mathfrak{p} \not\supseteq \mathfrak{a}\}.$$

La topología que definen los subconjuntos $\mathcal{V}(\mathfrak{a})$ se llama la **topología de Zariski**.

Soporte de un módulo

Para cada A–módulo M llamamos **soporte** de M a:

$$\operatorname{Supp}(M) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\}.$$

Lema. 42.22.
Sea A un anillo conmutativo y M un A–módulo. Son equivalentes los siguientes enunciados:
(a) $M = 0$;
(b) $\operatorname{Supp}(M) = \varnothing$.

Es consecuencia del Lema (42.16.).

Lema. 42.23.
Sea A un anillo conmutativo. Se verifica:
(1) Si $\mathfrak{a}$ es un ideal de A, entonces $\operatorname{Supp}(A/\mathfrak{a}) = \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \supseteq \mathfrak{a}\} = \mathcal{V}(\mathfrak{a})$;
(2) Si $0 \to M' \to M \to M'' \to 0$ *es una sucesión exacta, entonces* $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$;
(3) Si M es un A–módulo finitamente generado, entonces $\operatorname{Supp}(M) = \mathcal{V}(\operatorname{Ann}(M))$, *y por tanto* $\operatorname{Supp}(M)$ *es un subconjunto cerrado de* $\operatorname{Spec}(A)$;
(4) Si M y N son A–módulos finitamente generados, entonces $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$;
(5) Sea $\mathfrak{a}$ un ideal de A y M un A–módulo finitamente generado, entonces $\operatorname{Supp}(M/\mathfrak{a}M) = \mathcal{V}(\mathfrak{a} + \operatorname{Ann}(M))$.

DEMOSTRACIÓN.

(1) De la sucesión exacta $0 \to \mathfrak{a}_{\mathfrak{p}} \to A_{\mathfrak{p}} \to (A/\mathfrak{a})_{\mathfrak{p}} \to 0$ se deduce $\mathfrak{p} \in \operatorname{Supp}(A/\mathfrak{a})$ si y solo si $\mathfrak{a}_{\mathfrak{p}} \neq A_{\mathfrak{p}}$, si y solo si $\mathfrak{a} \cap (A \setminus \mathfrak{p}) = \varnothing$, si y solo si $\mathfrak{a} \subseteq \mathfrak{p}$.

(2) Es consecuencia de la exactitud del funtor localización.

(3) Sea $M = Am_1 + \cdots + Am_t$, entonces $M_{\mathfrak{p}} = (Am_1)_{\mathfrak{p}} + \cdots + (Am_t)_{\mathfrak{p}}$ para cada ideal primo $\mathfrak{p}$, entonces

$$\begin{aligned}\operatorname{Supp}(M) = \cup_{i=1}^t \operatorname{Supp}(Am_i) = \cup_{i=1}^t \operatorname{Supp}(A/(0:m_i)) &= \cup_{i=1}^t \mathcal{V}((0:m_i)) \\ &= \mathcal{V}(\cap_{i=1}^t (0:m_i)) = \mathcal{V}(0:M).\end{aligned}$$

(4) Primero probamos que si A es un anillo local con ideal maximal $\mathfrak{m}$ y M, N son A–módulos finitamente generados, entonces $M \otimes_A N \neq 0$.

Por el Lema de Nakayama $M/\mathfrak{m}M$ y $N/\mathfrak{m}N$ son no nulos, luego tenemos un epimorfismo

$$M \otimes_A N \longrightarrow M/\mathfrak{m}M \otimes_A N/\mathfrak{m}N \cong M/\mathfrak{m}M \otimes_{A/\mathfrak{m}} N/\mathfrak{m}N \neq 0$$

Sea ahora $\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N)$, entonces $0 \neq (M \otimes_A N)_\mathfrak{p} = M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p}$, luego $\mathfrak{p} \in \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$.

Sea $\mathfrak{p} \in \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$, entonces $0 \neq M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} \cong (M \otimes_A N)_\mathfrak{p}$ y por tanto $\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N)$.

(5) Como $M/(\mathfrak{a}M) \cong (A/\mathfrak{a}) \otimes_A M$, tenemos:

$$\operatorname{Supp}(M/(\mathfrak{a}M)) = \operatorname{Supp}(A/\mathfrak{a}) \cap \operatorname{Supp}(M) = \mathcal{V}(\mathfrak{a}) \cap \mathcal{V}(\operatorname{Ann}(M)) = \mathcal{V}(\mathfrak{a} + \operatorname{Ann}(M)).$$

□

43. Ejercicios

Localización

Ejercicio. 43.1. (AM, Cap 3, Ej 7)
Dado un anillo A, llamamos Σ_0 al conjunto de todos los no divisores de cero de A (los elementos regulares de A). Demuestra que Σ_0 es un conjunto multiplicativo saturado. El anillo de fracciones $\Sigma_0^{-1}A$ se llama el **anillo total de fracciones** *de A. Demuestra que:*

(1) Σ_0 es el mayor subconjunto multiplicativo saturado Σ de A tal que $\lambda_A : A \longrightarrow \Sigma^{-1}A$ es un homomorfismo inyectivo.
(2) Cada elemento de $\Sigma_0^{-1}A$ es un divisor de cero o un elemento invertible.

SOLUCIÓN

Ejercicio. 43.2.
¿Por qué al definir la relación de equivalencia $(a,b) \sim (c,d)$ en $A \times \Sigma$ tenemos que usar la definición: "existe $t \in \Sigma$ tal que $t(ad-bc) = 0$"?
Prueba, dando un ejemplo, que en general sin la mención a $t \in \Sigma$ no tendríamos una relación de equivalencia.

SOLUCIÓN

Ejercicio. 43.3.
Dado un anillo A y un elemento $a \in A$. Se verifica:

(1) $A_a \cong \frac{A[X]}{(aX-1)}$.
(2) Son equivalentes:
   (a) a es nilpotente.
   (b) $A_a = 0$.

SOLUCIÓN

Nota.*Observa que si K es un cuerpo y consideramos el anillo $K[X]$, el cuerpo de fracciones es $K(X)$, que es el anillo de fracciones de $K[X]$ con respecto al subconjunto multiplicativo $\Sigma = K[X] \setminus \{0\}$. Por otro lado, $K[X]_X$ es el anillo de fracciones de $K[X]$ con respecto al subconjunto multiplicativo $\{X^n \mid n \in \mathbb{N}\}$. Éste último se representa también como $K[X, X^{-1}]$.*

Ejercicio. 43.4.
Prueba que A no tiene elementos nilpotentes no nulos si para todo ideal primo $\mathfrak{p}$ el anillo $A_\mathfrak{p}$ no tiene elementos nilpotentes no nulos.

SOLUCIÓN

Ejercicio. 43.5.
Se considera el anillo $K[X]$ y un elemento $a \in K$. Sea $\mathfrak{m} = \mathfrak{m}_a = \{F \in K[X] \mid F(a) = 0\}$.

(1) Prueba que $\mathfrak{m}$ es un ideal maximal de $K[X]$.
(2) Sea $\Sigma = K[X] \setminus \mathfrak{m} = \{F \in K[X] \mid F(a) \neq 0\}$. Describir los elementos de $\Sigma^{-1}K[X]$.

SOLUCIÓN

Ejercicio. 43.6.
Sea A un anillo y Σ un subconjunto multiplicativo, y $\mathfrak{n} = 0^{ec}$. Si $p : A \to A/\mathfrak{n}$ es la proyección, prueba que para cada $s \in \Sigma$ se tiene que $p(s) \in A/\mathfrak{n}$ no es un divisor de cero.

SOLUCIÓN

Ejercicio. 43.7.
Sea A un anillo y $\Sigma \subseteq A$ un subconjunto multiplicativo tal que $\Sigma \subseteq \Sigma_0$. Para cada anillo intermedio $A \subseteq B \subseteq \Sigma^{-1}A$ se tiene $\Sigma^{-1}A = \Sigma^{-1}B$.

SOLUCIÓN

Ejercicio. 43.8.
Determina:

(1) El anillo total de fracciones de $\mathbb{Z}$.
(2) El anillo total de fracciones de $\mathbb{Z} \times \mathbb{Z}$.
(3) El anillo total de fracciones de $\mathbb{Z}_{12}$.

SOLUCIÓN

Ejercicio. 43.9.
Sea K un cuerpo, $A = \frac{K[X,Y]}{(XY)}$ y $x = \overline{X}$, $y = \overline{Y}$ las clases de X e Y respectivamente. Demuestra que se verifica:

(1) $x/1$ es invertible en A_x.
(2) $y/1 = 0$ en A_x.
(3) Definimos $f : K[X] \to A_x$ mediante $f(X) = x/1$. Entonces f es un homomorfismo de anillos. Se tiene $\operatorname{Im}(f) = K[x] \subseteq A_x$.
(4) f se factoriza por $K[X, X^{-1}]$.
(5) $A_x \cong K[X, X^{-1}]$.

SOLUCIÓN

Ejercicio. 43.10.
Sea K un cuerpo, X un conjunto no vacío y A el anillo de las funciones de X en K. Demuestra que se verifica:

(1) Para cada $x \in X$ el conjunto $\mathfrak{m}_x = \{f \in A \mid f(x) = 0\}$ es un ideal maximal de A.
(2) El localizado es $A_{\mathfrak{m}_x} = \{f/g \mid f, g \in A,\ g(x) \neq 0\}$.
(3) Cada elemento $f/g \in A_{\mathfrak{m}_x}$ se puede evaluar en x mediante: $(f/g)(x) = f(x)/g(x)$. Este conjunto se llama el **anillo de las funciones racionales** *sobre X con valores en K definidas en x.*

SOLUCIÓN

Ejercicio. 43.11.
Sea $f : A \to B$ un homomorfismo de anillos tal que B es un A–módulo finitamente generado. Si $a \in A$ es un elemento que no es nilpotente prueba que el homomorfismo $f_a : A_a \to B_{f(a)}$ hace que $B_{f(a)}$ sea un A_a–módulo finitamente generado.

SOLUCIÓN

Ejercicio. 43.12.
Sea $A \subseteq B$ una extensión de anillos tal que B es un A–módulo finitamente generado. Prueba que para cada ideal primo $\mathfrak{p} \subseteq A$ existe sólo un número finito de ideales primos $\mathfrak{q} \subseteq B$ tales que $\mathfrak{q} \cap A = \mathfrak{p}$.

SOLUCIÓN

Ejercicio. 43.13.
Sea K un cuerpo, $A = K[X]$ el anillo de polinomios, F el cuerpo de fracciones de A y $A \subseteq S \subseteq F$ es un anillo intermedio.

(1) Para cada ideal $\mathfrak{p} \subseteq A$ se tiene $\mathfrak{p}S = S$ ó $S \subseteq A_{\mathfrak{p}}$.
(2) Para cada $x/y \in S$ se tiene $((y) : x)S = S$, donde $((y) : x) = \{a \in A \mid ax \in (y)\}$.
(3) Existe un subconjunto multiplicativo $\Sigma \subseteq A$ tal que $S = \Sigma^{-1}A$.

SOLUCIÓN

Ejercicio. 43.14.
Con la misma notación del Ejercicio (43.13.).
Sea K un cuerpo, $A = K[X]$ el anillo de polinomios, F el cuerpo de fracciones de A y $A \subseteq S \subseteq F$ es un anillo intermedio.

(4) Tenemos que el complemento de Σ es la unión de los ideales $\{\mathfrak{q} \cap A \mid \mathfrak{q}$ es un ideal maximal de $S\}$.
(5) Para cada ideal maximal $\mathfrak{q} \subseteq S$, si $\mathfrak{p} = \mathfrak{q} \cap A$, se tiene $A_{\mathfrak{p}} = S_{\mathfrak{q}}$.
(6) Se tienen la identidad: $S = \cap\{A_{\mathfrak{q}\cap A} \mid \mathfrak{q}$ es un ideal maximal de $S\}$.

SOLUCIÓN

Ejercicio. 43.15.
Sea A un anillo, $\Sigma \subseteq A$ un subconjunto multiplicativo, y $\mathfrak{p} \subseteq A$ un ideal primo. Son equivalentes:

(a) $\mathfrak{p}\Sigma^{-1}A$ es un ideal maximal.
(b) $\mathfrak{p}$ es un ideal maximal entre los que no cortan a Σ.

SOLUCIÓN

Ejercicio. 43.16.
Sea A un anillo y $\mathfrak{a}, \mathfrak{b} \subseteq A$ ideales.

(1) Si $\mathfrak{b}$ es finitamente generado, prueba que $\Sigma^{-1}(\mathfrak{a} : \mathfrak{b}) = \Sigma^{-1}\mathfrak{a} : \Sigma^{-1}\mathfrak{b}$.
(2) Prueba que en general se tiene $\Sigma^{-1}(\mathfrak{a} : \mathfrak{b}) \subseteq \Sigma^{-1}\mathfrak{a} : \Sigma^{-1}\mathfrak{b}$, pero no la inclusión contraria.

SOLUCIÓN

Ejercicio. 43.17.
Sea $\mathfrak{n} = \operatorname{Nil}(A)$ el nil-radical del anillo A.

(1) Para cada $\Sigma \subseteq A$ multiplicativamente cerrado prueba que $\Sigma^{-1}\mathfrak{n} = \Sigma^{-1}\operatorname{Nil}(A) = \operatorname{Nil}(\Sigma^{-1}A)$.
(2) ¿Qué ocurre con $\operatorname{Jac}(A)$?

*Un anillo A con $\operatorname{Nil}(A) = 0$ se llama **anillo reducido**.*

(3) Prueba que "reducido" es una propiedad local, esto es, $\operatorname{Nil}(A) = 0$ si, y sólo si, $\operatorname{Nil}(A_{\mathfrak{p}}) = 0$ para cada ideal primo $\mathfrak{p} \subseteq A$.
(4) ¿Qué ocurre con los anillos A tales que $\operatorname{Jac}(A) = 0$?

SOLUCIÓN

Dominios de factorización única

Ejercicio. 43.18.
*Sea D un dominio, un elemento no nulo x se llama **irreducible** si no es invertible y en cada factorización $x = x_1x_2$ se tiene que x_1 o x_2 es invertible. Los elementos irreducibles en algunos textos se llaman **átomos**. En un dominio D un elemento no nulo p se llama **primo** si no es invertible y si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

(1) Demuestra que cada elemento primo es irreducible.
(2) Da un ejemplo de un elemento irreducible que no sea primo.

SOLUCIÓN

Ejercicio. 43.19.
*Un dominio D se llama **atómico** si cada elemento no nulo y no invertible es un producto de átomos (= elementos irreducibles). Prueba que si D es un dominio de integridad que verifica la CCA para ideales principales, entonces D es atómico. En particular todo dominio noetheriano es atómico.*

SOLUCIÓN

Ejercicio. 43.20.
*Un dominio D es un **dominio de factorización única** si cada elemento no nulo y no invertible se puede escribir como un producto de elementos primos. Como consecuencia todo DFU es un dominio atómico.*

(1) Demuestra que si un elemento no nulo y no invertible tiene una factorización en elementos primos, esta factorización es única.

(2) Demuestra que un dominio atómico es un dominio de factorización única si, y solo si, todo elemento irreducible es primo.
(3) Demuestra que un dominio atómico es un dominio de factorización única si, y solo si, las factorizaciones en irreducibles son únicas.
(4) Demuestra que no todo dominio de integridad noetheriano es un dominio de factorización única.

SOLUCIÓN

Ejercicio. 43.21.
Sea D un dominio. Demuestra que son equivalentes:

(a) D es un DFU.
(b) (1) cada elemento irreducible es primo y (2) D verifica la CCA para ideales principales.

SOLUCIÓN

Ejercicio. 43.22.
Sea D un dominio de integridad y $\Sigma \subseteq D$ un subconjunto multiplicativo.

(1) Demuestra que $\Sigma^{-1}D$ es un dominio de factorización única si D lo es.
(2) Demuestra que si D es atómico, Σ está formado por productos de primos y $\Sigma^{-1}D$ es un dominio de factorización única, entonces D es un dominio de factorización única.

SOLUCIÓN

Extensiones enteras

Ejercicio. 43.23.
Estudia los siguientes enunciados:

(1) Sea $A \subseteq B$ una extensión entera y $\Sigma \subseteq A$ un subconjunto multiplicativo. Prueba que $\Sigma^{-1}A \subseteq \Sigma^{-1}B$ es una extensión entera.
(2) Si $A \subseteq C \subseteq B$ es la clausura entera de A en B y $\Sigma \subseteq A$ un subconjunto multiplicativo. Prueba que la clausura $\Sigma^{-1}A$ en $\Sigma^{-1}B$ es $\Sigma^{-1}C$.

SOLUCIÓN

Ejercicio. 43.24.
Sea A un dominio normal y $\Sigma \subseteq A$ un subconjunto multiplicativo. Prueba que $\Sigma^{-1}A$ es un dominio normal.

SOLUCIÓN

Ejercicio. 43.25.
Sea A un dominio de integridad. Son equivalentes:

(a) A es normal.
(b) $A_{\mathfrak{p}}$ es normal para cada ideal primo $\mathfrak{p} \subseteq A$.
(c) $A_{\mathfrak{m}}$ es normal para cada ideal maximal $\mathfrak{m} \subseteq A$.

SOLUCIÓN

Localización de anillos finitos

Ejercicio. 43.26.
¿Es cierto que si $A_{\mathfrak{p}}$ es un dominio de integridad si para cada ideal primo $\mathfrak{p} \subseteq A$ el anillo $A_{\mathfrak{p}}$ es un dominio de integridad.

SOLUCIÓN

Ejercicio. 43.27.
Demuestra que para cualquier anillo conmutativo A los siguientes enunciados son equivalentes:

(a) Para todo ideal primo $\mathfrak{p}$, el anillo $A_{\mathfrak{p}}$ es un dominio de integridad.
(b) Para todo ideal maximal $\mathfrak{m}$, el anillo $A_{\mathfrak{m}}$ es un dominio de integridad.
(c) Para todos $a, b \in A$ si $ab = 0$, entonces $\operatorname{Ann}(a) + \operatorname{Ann}(b) = A$.

¿Es dominio de integridad una propiedad local?

SOLUCIÓN

Ejercicio. 43.28.
En el caso en que $D = \mathbb{Z}_6$ los dos únicos ideales primos son $\mathfrak{p}_2 = 2\mathbb{Z}_6$ y $\mathfrak{p}_3 = 3\mathbb{Z}_6$. Observar que en este caso se tiene $(\mathbb{Z}_6)_{\mathfrak{p}_2} \cong \mathbb{Z}_2$, y $(\mathbb{Z}_6)_{\mathfrak{p}_3} \cong \mathbb{Z}_3$.
Todas las localizaciones de $\mathbb{Z}_6$ son cuerpos, sin embargo $\mathbb{Z}_6$ no es ni siquiera un dominio de integridad.

SOLUCIÓN

Ejercicio. 43.29.
Sea $A = \mathbb{Z}/m\mathbb{Z}$. Demuestra que para cada subconjunto multiplicativo Σ de A existe un entero n tal que $\Sigma^{-1}A = \mathbb{Z}/n\mathbb{Z}$.

SOLUCIÓN

Ejercicio. 43.30.
Con la notación del ejercicio anterior. ¿Qué valores son posibles para n?

SOLUCIÓN

Subconjuntos saturados

Ejercicio. 43.31. (AM, Cap 3, Ej 7)
*Un subconjunto multiplicativo $\Sigma \subseteq A$ se llama **saturado** si verifica que $ab \in \Sigma$ implica $a \in \Sigma$ y $b \in \Sigma$ para cada $a, b \in A$.*

(1) Demuestra que un subconjunto multiplicativo $\Sigma \subseteq A$ es saturado si y solo si el complemento $A \setminus \Sigma$ es una unión de ideales primos.
*(2) Demuestra que para cada conjunto multiplicativo $\Sigma \subseteq A$ existe un único conjunto saturado mínimo $\overline{\Sigma}$ que contiene a Σ, y que coincide con el complemento en A de la unión de los ideales primos que no cortan a Σ. Llamamos a $\overline{\Sigma}$ la **saturación** de Σ.*
(3) Si $\Sigma = 1 + \mathfrak{a}$ para un ideal propio $\mathfrak{a}$, calcula la saturación de Σ.

SOLUCIÓN

Ejercicio. 43.32.
Sea A un anillo conmutativo y $\Sigma \subseteq A$ un subconjunto multiplicativo, si $\overline{\Sigma}$ es la saturación de Σ, demuestra que existe un único isomorfismo $f : \Sigma^{-1}A \longrightarrow \overline{\Sigma}^{-1}A$ que hace conmutar el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\lambda_\Sigma} & \Sigma^{-1}A \\ & {\scriptstyle\lambda_{\overline{\Sigma}}}\searrow \quad \swarrow{\scriptstyle f} & \\ & \overline{\Sigma}^{-1}A & \end{array}$$

SOLUCIÓN

Ejercicio. 43.33.
Recuerda que un conjunto multiplicativo $\Sigma \subseteq A$ se llama **saturado** *si $ab \in \Sigma$, entonces $a \in \Sigma$ y $b \in \Sigma$, para todos $a, b \in A$.*

(1) Si $\Sigma \subseteq A$ es saturado, entonces Σ contiene a todos los elementos $a \in A$ tales que $a/1 \in \Sigma^{-1}A$ es invertible.
(2) $\Sigma = \{1\} \subseteq \mathbb{Z}$ no es un conjunto multiplicativo saturado.

SOLUCIÓN

Ejercicio. 43.34.
Sea A un anillo conmutativo y sea $\mathfrak{p}$ un ideal primo de A. Demuestra que $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ es isomorfo al cuerpo de fracciones del dominio de integridad $A/\mathfrak{p}$.

SOLUCIÓN

Relaciones entre subconjuntos multiplicativos

Ejercicio. 43.35.
Sea A un anillo, $\Sigma \subseteq A$ un subconjunto multiplicativo, $\mathfrak{a} \subseteq A$ un ideal tal que $\mathfrak{a} \cap \Sigma = \varnothing$ y $p : A \longrightarrow A/\mathfrak{a}$ la proyección canónica. Demuestra que se verifica:

(1) $p(\Sigma)$ es un subconjunto multiplicativo de $A/\mathfrak{a}$.
(2) Existe un isomorfismo de anillos $\Sigma^{-1}A/\Sigma^{-1}\mathfrak{a} \cong p(\Sigma)^{-1}(A/\mathfrak{a})$.
(3) En el caso particular en el que $\mathfrak{p} \supseteq \mathfrak{a}$ es un ideal primo, se tiene $\Sigma = A \setminus \mathfrak{p}$ verifica estas condiciones, y por tanto se tiene un isomorfismo: $(A/\mathfrak{a})_{\mathfrak{p}/\mathfrak{a}} \cong A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}$.

SOLUCIÓN

Ejercicio. 43.36.
Sea $f : A \longrightarrow B$ un homomorfismo de anillos y $\Sigma \subseteq A$ un subconjunto multiplicativo de A tal que $\operatorname{Ker}(f) \cap \Sigma = \varnothing$. Demuestra:

(1) $f(\Sigma) \subseteq B$ es un subconjunto multiplicativo.
(2) Existe un homomorfismo de anillos $\Sigma^{-1}A \longrightarrow f(\Sigma)^{-1}B$ definido por $f(a/s) = f(a)/f(s)$ para cada $a/s \in \Sigma^{-1}A$.
(3) Existe un isomorfismo de A–módulos $\Sigma^{-1}B \cong f(\Sigma)^{-1}B$.

SOLUCIÓN

Ejercicio. 43.37. (AM, Cap 3, Ej 3)
Sea A un anillo conmutativo y $\Sigma, \Gamma \subseteq A$ subconjuntos multiplicativos. Sea $\lambda : A \longrightarrow \Sigma^{-1}A$ el homomorfismo canónico y $\Gamma_1 = \lambda(\Gamma)$. Demuestra que $\Gamma_1^{-1}(\Sigma^{-1}A) \cong (\Gamma\Sigma)^{-1}A$, donde $\Gamma\Sigma = \{ts \mid t \in \Gamma \text{ y } s \in \Sigma\}$.

SOLUCIÓN

Ejercicio. 43.38.
Sea A un anillo y $\Sigma_1, \Sigma_2 \subseteq A$ subconjuntos multiplicativos de A. Si llamamos Σ a la ***clausura multiplicativa*** *de $\Sigma_1 \cup \Sigma_2$ (el menor subconjunto multiplicativo que contiene a Σ_1 y Σ_2, entonces se tienen los isomorfismos*

$$\Sigma_1^{-1}\Sigma_2^{-1}A \cong \Sigma^{-1}A \cong \Sigma_2^{-1}\Sigma_1^{-1}A$$

SOLUCIÓN

Ejercicio. 43.39.
Sea $f : A \to B$ un homomorfismo de anillos, y $\Gamma \subseteq B$ un subconjunto multiplicativo. Definimos $\Sigma = \{a \in A \mid f(a) \in \Gamma\}$. Prueba:

(1) Σ es un subconjunto multiplicativo y $\operatorname{Ker}(f) \cap \Sigma = \varnothing$.
(2) Existe un único homomorfismo f' que hace conmutar el diagrama:

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle \lambda_{\Sigma,A}}\downarrow & & \downarrow{\scriptstyle \lambda_{\Gamma,B}} \\ \Sigma^{-1}A & \xrightarrow{\ f'\ } & \Gamma^{-1}B \end{array}$$

(3) Si f es sobreyectivo entonces f' es sobreyectiva y $\operatorname{Ker}(f') = \Sigma^{-1}\operatorname{Ker}(f)$.
(4) Si f es inyectivo, no necesariamente f' es inyectivo.

SOLUCIÓN

Ejercicio. 43.40.
Sea A un anillo y $\Sigma \subseteq A$ un subconjunto multiplicativo. Demuestra que se verifica:

(1) Si $\mathfrak{a} \subseteq A$ es un ideal, entonces $\mathfrak{a}^{ec} = \cup\{(\mathfrak{a} : s) \mid s \in \Sigma\}$, y en consecuencia $\mathfrak{a}^e = \Sigma^{-1}A$ si, y solo si, $\mathfrak{a} \cap \Sigma \neq \varnothing$.

(2) Un ideal $\mathfrak{a}$ de A es un contraído si, y solo si, ningún elemento de Σ es un divisor de cero en $A/\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 43.41.
Sea $f : A \to B$ un homomorfismo de anillos conmutativos, siendo cada ideal de B extendido de un ideal de A, y $\mathfrak{p}$ un ideal primo de A. Entonces $\mathfrak{p}$ es la contracción de un ideal primo de B si, y solo si, $\mathfrak{p}^{ec} = \mathfrak{p}$.

SOLUCIÓN

Propiedades de los anillos de fracciones

Ejercicio. 43.42.
Demostrar que para cada subanillo A de $\mathbb{Q}$ existe un subconjunto multiplicativo Σ de $\mathbb{Z}$ tal que $A = \Sigma^{-1}\mathbb{Z}$.

SOLUCIÓN

Ejercicio. 43.43.
Sea D un dominio de integridad y $\Sigma \subseteq D$ un subconjunto multiplicativo.

(1) Demuestra que $\Sigma^{-1}D$ es un subanillo del cuerpo de fracciones de D.
(2) Demuestra que si D es un dominio de ideales principales, también $\Sigma^{-1}D$ es un dominio de ideales principales.
(3) Demostrar que si D es un dominio de factorización única, también $\Sigma^{-1}D$ es un dominio de factorización única.
(4) Demostrar que si D es un dominio noetheriano, también $\Sigma^{-1}D$ es un dominio noetheriano.

SOLUCIÓN

Ejercicio. 43.44.
Prueba que A es un anillo (conmutativo) artiniano entonces para cada subconjunto multiplicativo $\Sigma \subseteq A$ el anillo $\Sigma^{-1}A$ es artiniano.
Da un ejemplo de que el recíproco no es cierto en general.

SOLUCIÓN

Ideales primos

Ejercicio. 43.45.
Prueba que el ideal $\mathfrak{p} = (Y^4 - Z^3, Y^2 - XZ, XY^2 - Z^2, X^2 - Z) \subseteq \mathbb{Q}[X, Y, Z]$ *es un ideal primo.*

SOLUCIÓN

Ejercicio. 43.46.
Prueba que el ideal $\mathfrak{p} = (XZ - X - Y^2 + 2Y + Z - 2, X^3 + 3X^2 + 3X - YZ + Y + Z, X^2Y - X^2 + 2XY - 2X + Y + 2Z - Z^2 - 2) \subseteq \mathbb{Q}[X, Y, Z]$ *es un ideal primo.*

SOLUCIÓN

Ejercicio. 43.47.
Estudia si es primo el ideal $\mathfrak{a} = (Y^4 - Z^3, Y^2 - XZ, XY^2 - Z^2, X^2 - Z) \subseteq \mathbb{C}[X, Y, Z]$.

SOLUCIÓN

Ejercicio. 43.48.
Estudia si es primo el ideal $\mathfrak{a} = (XZ - X - Y^2 + 2Y + Z - 2, X^3 + 3X^2 + 3X - YZ + Y + Z, X^2Y - X^2 + 2XY - 2X + Y + 2Z - Z^2 - 2) \subseteq \mathbb{C}[X, Y, Z]$.

SOLUCIÓN

Ejercicio. 43.49.
Estudia si el ideal $\mathfrak{a} = (XZ - Y^2, YZ - X^3, Z^2 - X^2Y)$ *es un ideal primo de* $\mathbb{C}[X, Y, Z]$.

SOLUCIÓN

Ejercicio. 43.50.
Sean $\mathfrak{a} = (X^3 + Y^3 + Z^3, X^2 + Y^2 + Z^2, X + Y + Z) \subseteq \mathbb{R}[X, Y, Z]$. *Prueba que* $\operatorname{rad}(\mathfrak{a}) = (X, Y, Z)$.

SOLUCIÓN

Ejercicio. 43.51.
Prueba que el ideal $\mathfrak{a} = (Y^3 - XZ, XY^2 - Z^2)$ no es primo en el anillo $\mathbb{Q}[X,Y,Z]$, y halla dos elementos $a, b \in \mathbb{Q}[X,Y,Z] \setminus \mathfrak{a}$ tales que $ab \in \mathfrak{a}$.

SOLUCIÓN

Módulos

Ejercicio. 43.52.
Sea A un dominio de integridad con cuerpo de fracciones K. Demuestra que $\cap\{A_\mathfrak{m} \mid \mathfrak{m} \subseteq A \text{ es maximal}\} = A$.
El mismo resultado es cierto si se toman los ideales primos.

SOLUCIÓN

Ejercicio. 43.53.
Sean $N_1, N_2 \subseteq M$ submódulos de un A–módulo M. Demuestra que $N_1 \subseteq N_2$ si y sólo si $(N_1)_\mathfrak{m} \subseteq (N_2)_\mathfrak{m}$ para cada ideal maximal $\mathfrak{m}$ de A.

SOLUCIÓN

Ejercicio. 43.54.
Sea $\Sigma \subseteq A$ un subconjunto multiplicativo y M un A–módulo finitamente generado. Demuestra que $\Sigma^{-1}M = 0$ si y solo si existe $s \in \Sigma$ tal que $sM = 0$.

SOLUCIÓN

Ejercicio. 43.55.
Sea A un dominio de integridad con cuerpo de fracciones K. Demostrar que K es un A–módulo finitamente generado si, y sólo si, $A = K$.

SOLUCIÓN

Ejercicio. 43.56.
Sea $\mathfrak{a} = (2X, 3Y) \subseteq \mathbb{Z}[X,Y]$. Calcula la saturación de $\mathfrak{a}$ respecto al conjunto multiplicativo $\Sigma = \mathbb{Z} \setminus \{0\}$.

SOLUCIÓN

Ejercicio. 43.57.
Un elemento $a \in A$ se llama **regular** *si $ab = 0$, entonces $b = 0$, esto es, a no es un divisor de cero.*

(1) Llamamos $\Sigma_0 = \Sigma_0(A)$ al conjunto de todos los elementos regulares de A. Prueba que Σ_0 es un subconjunto multiplicativamente cerrado saturado.
(2) Para cada A–módulo M definimos la **Σ_0–torsión** *de M como el núcleo del homomorfismo $\lambda : M \to \Sigma_0^{-1}M$. Prueba que la Σ_0–torsión de M es el submódulo $T_{\Sigma_0}(M) = \{m \in M \mid \exists s \in \Sigma_0$ tal que $sm = 0\}$.*
(3) Prueba que $T_{\Sigma_0}(A) = 0$, esto es, $\lambda : A \to \Sigma_0^{-1}A$ es una aplicación inyectiva.
(4) Prueba que para cada módulo M se tiene $T_{\Sigma_0}(M/T_{\Sigma_0}(M)) = 0$.
(5) Prueba que para cada familia de módulos $\{M_i \mid i \in A\}$ se tiene $T_{\Sigma_0}(\oplus_i M_i) = \oplus_i T_{\Sigma_0}(M_i)$.

SOLUCIÓN

Ejercicio. 43.58.
Sea A un dominio de integridad y M un A–módulo. Si para cada ideal maximal $\mathfrak{m} \subseteq A$ la localización $M_\mathfrak{m}$ es un $A_\mathfrak{m}$–módulo libre de torsión, prueba que M es un A–módulo libre de torsión.

SOLUCIÓN

Anillos artinianos

Ejercicio. 43.59.
Sea Σ un subconjunto multiplicativo del anillo $A = A_1 \times \cdots \times A_t$ con proyecciones $p_i A \to A_i$, $i = 1, \ldots, t$.

(1) Prueba que $\Sigma^{-1}A \cong p_1(\Sigma)^{-1}A_1 \times \cdots \times p_t(\Sigma)^{-1}A_t$.
(2) Si A es un anillo artiniano y $\Sigma \subseteq A$ un subconjunto multiplicativo, prueba que el homomorfismo $\Lambda : A \to \Sigma^{-1}A$ es sobreyectivo.

SOLUCIÓN

Capítulo VIII

Dimensión

Introducción

Una vez que hemos construido un invariante algebraico: la dimensión, en este capítulo vamos a estudiar los anillos y álgebras de dimensiones bajas. Primero establecemos algunos resultados sobre anillos noetherianos, para posteriormente caracterizar los anillos artinianos como los anillos noetherianos de dimensión cero. Establecemos un teorema de estructura para anillos artinianos: cada anillo artiniano es un producto directo finito de anillos artinianos locales. Finalizamos el capítulo estudiando ejemplos de anillos de dimensiones varias.

44. Anillos noetherianos

Anillos noetherianos

Veamos algunos resultados sobre la construcción de ideales primos en anillos, y especialmente en anillos noetherianos.

Lema. 44.1.
Sea A un anillo conmutativo y M un A–módulo. Si $\mathfrak{a}$ es un ideal de A, maximal entre los anuladores de elementos no nulos de M, entonces $\mathfrak{a}$ es un ideal primo de A.

DEMOSTRACIÓN. Sea $\mathfrak{a}$ un ideal maximal entre los anuladores de elementos no nulos de M y sean $a, b \in A$ tales que $ab \in \mathfrak{a}$. Finalmente sea $0 \neq m \in M$ tal que $\mathfrak{a} = \operatorname{Ann}(m)$. Si $b \notin \mathfrak{a}$ se tiene $bm \neq 0$ y como $\mathfrak{a} + Aa \subseteq \operatorname{Ann}(bm)$, la maximalidad de $\mathfrak{a}$ fuerza a que $\mathfrak{a} = \mathfrak{a} + Aa$, luego $a \in \mathfrak{a}$. □

Lema. 44.2.
Sea A un anillo conmutativo. Para cada cadena $\{\mathfrak{p}_\alpha \mid \alpha \in \Lambda\}$ de ideales primos se verifica que $\cup_\alpha \mathfrak{p}_\alpha$ y $\cap_\alpha \mathfrak{p}_\alpha$ son ideales primos.

DEMOSTRACIÓN. (1). $\cup_\alpha \mathfrak{p}_\alpha$ es un ideal primo. Sean $a, b \in A$ tales que $ab \in \cup_\alpha \mathfrak{p}_\alpha$, existen un índice β tal que $ab \in \mathfrak{p}_\beta$, luego $a \in \mathfrak{p}_\beta$ o $b \in \mathfrak{p}_\beta$, y tenemos el resultado. par (2). $\cap_\alpha \mathfrak{p}_\alpha$ es un ideal primo. Sean $a, b \in A$ tales que $ab \in \cap_\alpha \mathfrak{p}_\alpha$, si $a \notin \cap_\alpha \mathfrak{p}_\alpha$, existe un índice β tal que $a \notin \mathfrak{p}_\beta$, pero entonces $a \notin \mathfrak{p}_\gamma$ para cada $\gamma \geq \beta$, y como $ab \in \mathfrak{p}_\gamma$, y éste es primo, resulta $b \in \mathfrak{p}_\gamma$. Por lo tanto $b \in \cap_\alpha \mathfrak{p}_\alpha$. □

Lema. 44.3.
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal propio de A, existe un ideal primo $\mathfrak{p}$ de A que es minimal sobre $\mathfrak{a}$.

DEMOSTRACIÓN. Por ser $\mathfrak{a}$ propio tenemos que existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{a} \subseteq \mathfrak{m}$, y por tanto la familia

$$\Gamma = \{\mathfrak{p} \mid \mathfrak{p} \text{ es primo y } \mathfrak{p} \supseteq \mathfrak{a}\}$$

es no vacía. Dada una cadena descendente en Γ:

$$\mathfrak{p}_1 \supseteq \mathfrak{p}_2 \supseteq \cdots ,$$

llamamos $\mathfrak{p} = \cap_\alpha \mathfrak{p}_\alpha$. Por el Lema (44.2.) tenemos que $\mathfrak{p}$ es un ideal primo, y por tanto en Γ existirán elementos minimales. □

Proposición. 44.4.
Si A es un anillo noetheriano, existe sólo un número finito de ideales primos minimales.

DEMOSTRACIÓN. Supongamos que el resultado no se verifica. Definimos Γ como a la familia de los ideales de A que no tienen un conjunto finito de ideales primos minimales. Por la hipótesis resulta que $\Gamma \neq \varnothing$. Por ser A noetheriano podemos tomar $\mathfrak{a} \in \Gamma$ maximal. Resulta que si cambiamos A por $A/\mathfrak{a}$, entonces A no tiene un número finito de ideales primos minimales, pero cada ideal propio no nulo de A sí tiene un número finito de ideales primos minimales.

Como A no es un dominio, sean $\mathfrak{a}$, $\mathfrak{b}$ ideales no nulos de A tales que $\mathfrak{ab} = 0$, entonces para cada ideal primo minimal $\mathfrak{p}$ de A se verifica $\mathfrak{ab} \subseteq \mathfrak{p}$, luego $\mathfrak{a} \subseteq \mathfrak{p}$ ó $\mathfrak{b} \subseteq \mathfrak{p}$. En cualquier caso resulta que $\mathfrak{p}$ es minimal sobre $\mathfrak{a}$ ó sobre $\mathfrak{b}$. En consecuencia existe un número finito de ideales primos minimales, lo que es una contradicción. □

Corolario. 44.5.
Si A es un anillo noetheriano, sobre cada ideal propio $\mathfrak{a}$ de A sólo existe un número finito de ideales primos minimales sobre $\mathfrak{a}$.

Lema. 44.6.
En un anillo noetheriano el nilradical es nilpotente.

DEMOSTRACIÓN. Como A es noetheriano resulta que $\mathrm{Nil}(A)$ es un ideal finitamente generado. Sea $\mathrm{Nil}(A) = a_1A + \cdots + a_sA$. Para cada índice i existe $n_i \in \mathbb{N}$ tal que $a_i^{n_i} = 0$, tomamos $n = \max\{n_1, \ldots, n_s\}$. Un sistema de generadores de $\mathrm{Nil}(A)^{sn}$ está formado por los elementos $a_1^{e_1} \cdots a_s^{e_s}$, con $e_1 + \cdots + e_s = sn$. En consecuencia algún e_i es mayor ó igual que n y por tanto $a_1^{e_1} \cdots a_s^{e_s} = 0$. Luego $\mathrm{Nil}(A)^{sn} = 0$. □

Corolario. 44.7.
En un anillo noetheriano cada ideal contiene una potencia de su radical.

45. Anillos artinianos

Estudiamos a continuación los ideales primos en anillos artinianos.

Proposición. 45.1.
En un anillo artiniano cada ideal primo es maximal.

DEMOSTRACIÓN. Sea $\mathfrak{p}$ un ideal primo de A, entonces $A/\mathfrak{p}$ es un dominio de integridad artiniano. Dado $0 \neq x \in A/\mathfrak{p}$, consideramos la cadena descendente de ideales:

$$x(A/\mathfrak{p}) \supseteq x^2(A/\mathfrak{p}) \supseteq \cdots .$$

Existe entonces $n \in \mathbb{N}$ tal que $x^n(A/\mathfrak{p}) = x^{n+1}(A/\mathfrak{p})$. Resulta que existe $y \in A/\mathfrak{p}$ tal que $x^n = x^{n+1}y$, luego $1 = xy$ y por tanto x es una unidad y $A/\mathfrak{p}$ es un cuerpo. □

Corolario. 45.2.
Si A es un anillo artiniano, $\mathrm{Nil}(A) = \mathrm{Jac}(A)$.

DEMOSTRACIÓN. Recordar que $\mathrm{Nil}(A)$ es la intersección de todos los ideales primos y $\mathrm{Jac}(A)$ es la intersección de todos los ideales maximales. Como cada ideal primo es maximal, se tiene el resultado. □

Proposición. 45.3.
En un anillo artiniano existe sólo un número finito de ideales primos.

DEMOSTRACIÓN. Consideramos Γ el conjunto de todas las intersecciones finitas de ideales primos, y por tanto maximales, de A. Como A es un anillo artiniano, resulta que Γ tiene un elemento minimal. Sea $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t \in \Gamma$ minimal. Para cada ideal maximal $\mathfrak{m}$ tenemos:

$$\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t \subseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t,$$

luego por la minimalidad resulta

$$\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t \subseteq \mathfrak{m},$$

y por tanto $\mathfrak{m}$ es igual a uno de los $\mathfrak{m}_i$, $1 \leq i \leq t$. □

Corolario. 45.4.
En un anillo artiniano el nilradical es el producto de los ideales maximales.

DEMOSTRACIÓN. Es consecuencia de que los ideales maximales son un número finito, coinciden con los ideales primos y son comaximales. □

Corolario. 45.5.
Si A es un anillo artiniano, el cociente $A/\operatorname{Jac}(A)$ es isomorfo a un producto de cuerpos.

DEMOSTRACIÓN. Existe un número finito de ideales primos, y cada uno de ellos es maximal. Sean éstos $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$. Se tiene $\operatorname{Jac}(A) = \mathfrak{m}_1 \cap \ldots \cap \mathfrak{m}_t$, y por el Teorema Chino del Resto, existe un isomorfismo

$$A/\operatorname{Jac}(A) \cong A/\mathfrak{m}_1 \times \cdots \times A/\mathfrak{m}_t.$$

□

Proposición. 45.6.
En un anillo artiniano el nilradical es nilpotente.

DEMOSTRACIÓN. Supongamos que $\mathfrak{n} = \operatorname{Nil}(A)$. Por ser A artiniano, existe $n \in \mathbb{N}$ tal que $\mathfrak{n}^n = \mathfrak{n}^{n+1}$. Supongamos que $\mathfrak{n}^n \neq 0$.
Llamamos Γ al conjunto

$$\Gamma = \{\mathfrak{a} \subseteq A \mid \ \mathfrak{a}\mathfrak{n}^n \neq 0\},$$

por la suposición anterior tenemos que $\Gamma \neq \varnothing$. Otra vez por ser A artiniano, existe $\mathfrak{a} \in \Gamma$ minimal. Sea $a \in \mathfrak{a}$ tal que $a\mathfrak{n}^n \neq 0$, entonces por la minimalidad de $\mathfrak{a}$ tenemos que $\mathfrak{a} = aA$. También se verifica la relación

$$a\mathfrak{n}\mathfrak{n}^n = a\mathfrak{n}^{n+1} = a\mathfrak{n}^n \neq 0,$$

y por la minimalidad tenemos $a\mathfrak{n} = aA$. Entonces existe $y \in \mathfrak{n}$ tal que $ay = a$, y es fácil ver que se tiene $ay^s = a$ para cada $s \in \mathbb{N}$. Ahora bien, y es nilpotente, ya que $y \in \mathfrak{n}$, luego existe s tal que $y^s = 0$, y por tanto $a = 0$, lo que es una contradicción. □

Teorema. 45.7. (Teorema de Akizuki)
Todo anillo artiniano es noetheriano.

DEMOSTRACIÓN. Sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$ los ideales maximales de A y consideremos la siguiente cadena de submódulos:

$$A \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_t = \mathfrak{a} \supseteq \mathfrak{a}\mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{a}_1^n = 0$$

Cada cociente de esta cadena es de la forma $\mathfrak{b}/\mathfrak{b}\mathfrak{m}_i$, y por tanto es un $A/\mathfrak{m}_i$–módulo, esto es, un $A/\mathfrak{m}_i$–espacio vectorial y, como A es artiniano, resulta ser de dimensión finita. Podemos encontrar entonces una serie de composición de $\mathfrak{b}/\mathfrak{b}\mathfrak{m}_i$ (como $A/\mathfrak{m}_i$–espacio vectorial y como A–módulo). Entonces A tiene longitud finita y como consecuencia es un anillo noetheriano. □

El siguiente problema es ver qué condiciones es necesario añadir a un anillo noetheriano para que sea artiniano.
Para hacer el recíproco del Teorema de Akizuki, vamos a hacer el siguiente Lema.

Lema. 45.8.
Sea A un anillo en el que el ideal cero es un producto de ideales maximales, por ejemplo $\mathfrak{m}_1, \ldots, \mathfrak{m}_t$, no necesariamente distintos, entonces son equivalentes:
(a) A es un anillo noetheriano.
(b) A es un anillo artiniano.

DEMOSTRACIÓN. (a)⇒(b). Como tenemos $\mathfrak{m}_1 \cdots \mathfrak{m}_t = 0$, consideramos la cadena de submódulos:

$$A \supseteq \mathfrak{m}_1 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_t = 0,$$

entonces $\mathfrak{m}_1 \cdots \mathfrak{m}_s/\mathfrak{m}_1 \cdots \mathfrak{m}_{s+1}$ es un $A/\mathfrak{m}_{s+1}$–espacio vectorial de dimensión finita, esto es consecuencia de que A es un anillo noetheriano y de que $A/\mathfrak{m}_{s+1}$ es un cuerpo. Como consecuencia A es de longitud finita y por tanto A es un anillo artiniano. □

El siguiente resultado es un recíproco del Teorema de Akizuki.

Teorema. 45.9. (Teorema de Akizuki)
Sea A un anillo. Son equivalentes los siguientes enunciados:
(a) A es un anillo noetheriano y cada ideal primo es maximal;
(b) A es un anillo artiniano.

DEMOSTRACIÓN. (a)⇒(b). Por ser A un anillo noetheriano, existe un número finito de ideales primos minimales, luego $\mathrm{Nil}(A) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t$ para una familia finita de ideales maximales, ya que cada ideal primo, por la hipótesis, es maximal. Por ser $\mathrm{Nil}(A)$ nilpotente existe un entero positivo n tal que $\mathrm{Nil}(A)^n = 0$, entonces

$$(\mathfrak{m}_1 \cdots \mathfrak{m}_t)^n \subseteq (\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_t)^n = \mathrm{Nil}(A)^n = 0,$$

y aplicando el Lema anterior tenemos el resultado. □

El siguiente ejemplo muestra un anillo con un único ideal primo, y por tanto un único ideal maximal, que no es necesariamente artiniano y tampoco noetheriano.

Ejemplo. 45.10.
Sea K un cuerpo, $B = K[X_1, X_2, \ldots]$ el anillo en infinitas indeterminadas, $\mathfrak{b} = (X_1, X_2^2, X_3^3, \ldots)$, y $A := B/\mathfrak{b} = K[X_1, X_2, \ldots]/(X_1, X_2^2, X_3^3, \ldots)$ el anillo cociente.
Llamamos x_i a la clase de X_i. El anillo A tiene un único ideal primo, el ideal $\mathfrak{p} := (x_1, x_2, \ldots)$, que es maximal, ya que $A/\mathfrak{p} \cong K$ es un cuerpo. Sin embargo A no es un anillo noetheriano, ya que el ideal $\mathfrak{p}$ no es finitamente generado, y por tanto no es artiniano.

Módulos sobre anillos artinianos

Veamos algunas consecuencias de los Teoremas de Akizuki. El primer resultado es bien conocido.

Corolario. 45.11.
Sea A un anillo noetheriano y $\mathfrak{a}$ un ideal de A. Son equivalentes los siguientes enunciados:

(a) Todo ideal primo de A que contiene a $\mathfrak{a}$ es maximal;
(b) $A/\mathfrak{a}$ es un A–módulo de longitud finita;
(c) Todo ideal primo de $A/\mathfrak{a}$ es maximal;
(d) $\mathfrak{a}$ es un producto de ideales maximales.

Traducido a módulos tenemos una caracterización de los módulos de longitud finita en términos de ideales primos:

Corolario. 45.12.
Sea A un anillo noetheriano y M un A–módulo finitamente generado. Son equivalentes los siguientes enunciados:

(a) M es de longitud finita;
(b) Todo ideal primo de $\mathrm{Supp}(M)$ es maximal.

DEMOSTRACIÓN. (a)⇒(b). Si M es de longitud finita, entonces tiene una serie de composición

$$0 = M_0 \subset \cdots \subset M_r = M,$$

con ideales maximales $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ tales que $\mathfrak{m}_i = \operatorname{Ann}(M_i/M_{i-1})$. Tenemos $\operatorname{Ass}(M) \subseteq \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ está formado por ideales maximales, y como $\operatorname{Ass}(M)$ son los elementos minimales del soporte, resulta que el soporte está formado por ideales maximales.

(b)⇒(a). Consideremos una cadena

$$0 = M_0 \subset \cdots \subset M_r = M,$$

con $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ y $\mathfrak{p}_i \in \operatorname{Ass}(M) = \operatorname{Supp}(M)$ por verificarse (b). Entonces tenemos una serie de composición de M. □

Cuando el anillo es artiniano los módulos de longitud finita se caracterizan fácilmente.

Corolario. 45.13.
Sea A un anillo artiniano y M un A–módulo. Son equivalentes los siguientes enunciados:

(a) M es de longitud finita;
(b) M es finitamente generado.

En este caso tenemos $\operatorname{Ass}(M) = \operatorname{Supp}(M)$.

DEMOSTRACIÓN. Tenemos que A es un anillo noetheriano, entonces M es un A–módulo noetheriano y artiniano, luego de longitud finita. Como A es artiniano, todo ideal primo es maximal, y como $\operatorname{Ass}(M)$ son los elementos minimales de $\operatorname{Supp}(M)$, resulta que $\operatorname{Supp}(M) = \operatorname{Ass}(M)$. □

Corolario. 45.14.
Sea A un anillo noetheriano y M un A–módulo finitamente generado. Son equivalentes los siguientes enunciados:

(a) M es de longitud finita.
(b) $A/\operatorname{Ann}(M)$ es un anillo artiniano.

DEMOSTRACIÓN. Utilizando el Corolario (45.12.) basta probar que son equivalentes que el anillo $A/\operatorname{Ann}(M)$ es artiniano y que $\operatorname{Supp}(M)$ está formado por ideales maximales, y esto es equivalente a probar que los ideales que contienen a $\operatorname{Ann}(M)$ son maximales y son un número finito. □

Teorema de estructura de anillos artinianos

Los anillos artinianos tienen una estructura que se puede describir facilmente.

Teorema. 45.15. (Teorema de estructura de anillos artinianos)
Sea A un anillo artiniano con ideales maximales $\mathfrak{m}_1,\ldots,\mathfrak{m}_t$. Entonces A es isomorfo al anillo producto

$$A/\mathfrak{m}_1^{n_1}\times\cdots\times A/\mathfrak{m}_t^{n_t},$$

para algún $(n_1,\ldots,n_t)\in\mathbb{N}^t$. Además, cada $A/\mathfrak{m}_i^{n_i}$ es un anillo local artiniano con ideal maximal $\mathfrak{m}_i/\mathfrak{m}_i^{n_i}$.

DEMOSTRACIÓN. Tenemos $\operatorname{Nil}(A)=\mathfrak{m}_1\cdots\mathfrak{m}_t$. Existe $n\in\mathbb{N}$ tal que $0=\operatorname{Nil}(A)^n=\mathfrak{m}_1^n\cdots\mathfrak{m}_t^n$. Como los ideales $\mathfrak{m}_i^n$ son comaximales, resulta que $\mathfrak{m}_1^n\cdots\mathfrak{m}_t^n=\mathfrak{m}_1^n\cap\cdots\cap\mathfrak{m}_t^n$. Entonces por el Teorema Chino del Resto tenemos un isomorfismo

$$A\cong A/\operatorname{Nil}(A)^n\cong\frac{A}{\mathfrak{m}_1^n}\times\cdots\times\frac{A}{\mathfrak{m}_t^n}.$$

Los anillos $A/\mathfrak{m}_i^n$ son artinianos y $\mathfrak{m}_i/\mathfrak{m}_i^n$ es un ideal maximal, y como es nilpotente es el único. □

Ejemplo. 45.16.
Para cada $n\in\mathbb{Z}$ el anillo $\mathbb{Z}_n$ es finito, y por lo tanto es artiniano. Si la factorización de n es $n=p_1^{e_1}\cdots p_t^{e_t}$, entonces la descomposición de $\mathbb{Z}_n$ en producto de anillos artinianos locales es:

$$\mathbb{Z}_n=\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\times\cdots\times\frac{\mathbb{Z}}{p_t^{e_t}\mathbb{Z}}.$$

En efecto, el nilradical es $\mathfrak{n}:=\operatorname{Nil}(\mathbb{Z}_n)=p_1\cdots p_t\mathbb{Z}/n\mathbb{Z}=(p_1\mathbb{Z}/n\mathbb{Z})\cdots(p_t\mathbb{Z}/n\mathbb{Z})$, y se tiene $\mathfrak{n}^e=0$, siendo $e=\max\{e_1,\ldots,e_t\}$. Por tanto en aplicación del Teorema (45.15.) resulta

$$\mathbb{Z}_n\cong\frac{\mathbb{Z}/n\mathbb{Z}}{p_1^e\mathbb{Z}/n\mathbb{Z}}\times\cdots\times\frac{\mathbb{Z}/n\mathbb{Z}}{p_t^e\mathbb{Z}/n\mathbb{Z}}\cong\frac{\mathbb{Z}}{p_1^e\mathbb{Z}}\times\cdots\times\frac{\mathbb{Z}}{p_t^e\mathbb{Z}}=\frac{\mathbb{Z}}{p_1^{e_1}\mathbb{Z}}\times\cdots\times\frac{\mathbb{Z}}{p_t^{e_t}\mathbb{Z}}.$$

Ejemplo. 45.17.
El caso de un anillo cociente $K[X]/(F)$, siendo $F\in K[X]$ un polinomio no constante se resuelve de la misma forma, ya que en este caso $K[X]/(F)$ es una K–álgebra de dimensión finita, y por tanto las cadenas estrictas de ideales son finitas. Si la factorización de F es en polinomios irreducibles no asociados es

$$F=F_1^{e_1}\cdots F_t^{e_t},$$

entonces se tiene un isomorfismo

$$K[X]/(F)\cong\frac{K[X]}{(F_1^{e_1})}\times\cdots\times\frac{K[X]}{(F_t^{e_t})}.$$

Queda ahora el problema de determinar la estructura de los anillos locales artinianos.

Teorema. 45.18. (Estructura de anillos locales artinianos)
Sea A un anillo local noetheriano. Son equivalentes los siguientes enunciados:
(a) A es un anillo artiniano;
(b) El ideal maximal es nilpotente.

DEMOSTRACIÓN. (a)⇒(b). Si A es un anillo artiniano, entonces cada ideal primo es maximal y el nilradical es nilpotente, luego el único ideal maximal es nilpotente.
(b)⇒(a). Si el ideal maximal $\mathfrak{m}$ es un ideal nilpotente, entonces para cada ideal primo $\mathfrak{p}$ de A existe $n \in \mathbb{N}$ tal que $\mathfrak{m}^n \subseteq \mathfrak{p}$, entonces $\mathfrak{m} \subseteq \mathfrak{p}$, y por tanto $\mathfrak{m}$ es el único ideal maximal. Aplicando entonces el Teorema de Akizuki tenemos que A es un anillo artiniano. □

Vamos a estudiar con más detalle los anillos locales artinianos. Veamos antes un resultado sobre anillos locales noetherianos:

Lema. 45.19.
Sea A un anillo local noetheriano con ideal maximal $\mathfrak{m}$, se verifica una de las dos posibilidades siguientes:
(a) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ para cada $n \in \mathbb{N}$;
(b) $\mathfrak{m}^n = 0$ para algún $n \in \mathbb{N}$, y en este caso A es artiniano.

DEMOSTRACIÓN. Supongamos que existe $n \in \mathbb{N}$ tal que $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, entonces se tiene $\mathfrak{m}\mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}^n$, y por el Lema de Nakayama $\mathfrak{m}^n = 0$. Para ver que A es artiniano basta aplicar que el ideal cero es un producto de ideales maximales. □

Proposición. 45.20.
Sea A un anillo local artiniano con ideal maximal $\mathfrak{m}$ y cuerpo residual $K = A/\mathfrak{m}$. Son equivalentes los siguientes enunciados:
(a) Cada ideal de A es principal;
(b) El ideal maximal de A es principal;
(c) $\dim_K(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

DEMOSTRACIÓN. De forma evidente tenemos (a)⇒(b)⇒(c). Para probar que (c)⇒(a), supongamos que $\dim_K(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. Si $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 0$, entonces $\mathfrak{m} = \mathfrak{m}^2$, y por el Lema de Nakayama tenemos $\mathfrak{m} = 0$, entonces A es un cuerpo y se tiene el resultado. Si $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$, entonces tenemos que $\mathfrak{m}$ es un ideal principal. Supongamos que $\mathfrak{m} = xA$. Para cada ideal propio no nulo $\mathfrak{a} \subseteq A$ tenemos que $\mathfrak{a} \subseteq \mathfrak{m}$.

Ya que $\text{Nil}(A) = \mathfrak{m}$ es nilpotente, existe $m \in \mathbb{N}$ tal que $\mathfrak{a} \subseteq \mathfrak{m}^m = x^m A$ y $\mathfrak{a} \nsubseteq \mathfrak{m}^{n+1} = x^{m+1}A$. Entonces podemos tomar $y \in \mathfrak{a}$ de forma que $y = rx^m$ e $y \notin x^{m+1}A$, luego $r \notin xA = \mathfrak{m}$, esto es, es una unidad. Entonces $x^m \in yA \subseteq \mathfrak{a}$ y tenemos que $\mathfrak{a} = x^m A = \mathfrak{m}^m$ es un ideal principal. □

Estos últimos resultados nos dicen que los anillos locales artinianos conmutativos, a pesar de su simplicidad aparente son de complicada estructura: por un lado tenemos los anillos artinianos cuyos ideales son principales, ejemplo de éstos son:

(1) El anillo $\mathbb{Z}_{p^n}$ es un ejemplo de anillo local artiniano, en él cada ideal es principal.
(2) El mismo resultado se tiene al considerar el anillo local artiniano $K[X]/(F^e)$, siendo $F \in K[X]$ un polinomio irreducible.

Por otro lado aquellos cuyo ideal maximal no es principal.

(1) En el anillo $K[X^2, X^3]/(X^4) = K[x^2, x^3]$ el ideal maximal es (x^2, x^3). Por tanto no es un ideal principal. Además, se tiene que $\mathfrak{m}^2 = 0$, y $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 2$.

46. Repaso sobre la dimensión de anillos

Los anillos artinianos son anillos que tienen dimensión de Krull igual a cero, y en ellos las cadenas de ideales primos se reducen a un único elemento, pues todo ideal primo es maximal. En general no todo anillo de dimensión cero es un anillo artiniano.

Ejemplo. 46.1.
Se considera el anillo $A = \prod_{\mathbb{N}} \mathbb{Q} = \mathbb{Q}^{\mathbb{N}}$. Este anillo no es noetheriano y no es artiniano, ya que existe una cadena descendente no acotada:

$$\prod_{n\geq 0} \mathbb{Q} \supseteq \prod_{n\geq 1} \mathbb{Q} \supseteq \prod_{n\geq 2} \mathbb{Q} \supseteq \prod_{n\geq 3} \mathbb{Q} \supseteq \cdots$$

Sin embargo A es de dimensión cero, ya que los ideales primos son de la forma $\prod_{n\neq i} \mathbb{Q}$ para $i \in \mathbb{N}$, y los que contienen a $\oplus_{\mathbb{N}}\mathbb{Q}$; todos ellos son maximales.

Vamos a reunir en la siguiente proposición algunos resultados sobre anillos locales noetherianos.

Proposición. 46.2.
Sea A un anillo local noetheriano con ideal maximal $\mathfrak{m}$ y cuerpo residual $F = A/\mathfrak{m}$. Se verifica:

(1) El cociente $\mathfrak{m}/\mathfrak{m}^2$ es un F–espacio vectorial de dimensión finita. Sea $d := \dim_F(\mathfrak{m}/\mathfrak{m}^2)$.
(2) Todo conjunto de generadores de $\mathfrak{m}$ tiene al menos d elementos.
(3) Existe un conjunto de generadores de $\mathfrak{m}$ que tiene d elementos.
(4) $\dim_F(\mathfrak{m}/\mathfrak{m}^2) \geq \dim(A)$.
(5) En el caso en que $A := K[X_1, \ldots, X_n]_{(X_1,\ldots,X_n)}$, el localizado del anillo de polinomios en el ideal maximal $(X_1, \ldots, X_n)$, y $\mathfrak{m}$ el ideal maximal de A, se tiene

$$\dim_F(\mathfrak{m}/\mathfrak{m}^2) = n = \dim(A).$$

El anillo $A := K[X_1, \ldots, X_n]_{(X_1,\ldots,X_n)}$ proporciona un tipo especial de anillos, los anillos locales regulares. Un anillo noetheriano local A con ideal maximal $\mathfrak{m}$ se llama **regular** si verifica:

$$\dim_F(\mathfrak{m}/\mathfrak{m}^2) = \dim(A).$$

Recordemos que dado un ideal primo $\mathfrak{p}$ de un anillo A, la **altura** $\operatorname{ht}(\mathfrak{p})$ de $\mathfrak{p}$ es el supremo de las longitudes de las cadenas de ideales primos

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}$$

Y que en general se define al altura, $\operatorname{ht}(\mathfrak{a})$, de un ideal $\mathfrak{a}$ como el mínimo de las altura de los ideales primos minimales sobre $\mathfrak{a}$.

Proposición. 46.3.
Para cada ideal primo $\mathfrak{p}$ se verifica ht$(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$.

Proposición. 46.4.
Si A es un anillo noetheriano, entonces todo ideal primo de A tiene altura finita. En consecuencia el conjunto de los ideales primos de A verifica la condición de cadena descendente.

El concepto dual de altura es el de co–altura, a veces también llamado profundidad. La **co–altura** de un ideal primo $\mathfrak{p}$ en un anillo A se define como el supremo de las longitudes de las cadenas de ideales primos

$$\mathfrak{p} = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n.$$

Utilizamos la notación $\text{cht}(\mathfrak{p})$ para indicar la co–altura del ideal $\mathfrak{p}$.

Proposición. 46.5.
Para cada ideal primo $\mathfrak{p}$ se verifica cht$(\mathfrak{p}) = \dim(A/\mathfrak{p})$.

Veamos un ejemplo de un anillo noetheriano de dimensión infinita, en él hay ideales primos de altura arbitrariamente grande.

Ejemplo. 46.6. (Nagata)
Sea K un cuerpo y $B = K[X_1, X_2, \ldots]$ el anillo de polinomios en infinitas indeterminadas. Consideramos una sucesión creciente en enteros positivos: $1 = m_1 < m_2 < \cdots$ verificando que para cada índice i se tiene $0 < m_i - m_{i-1} < m_{i+1} - m_i$, y sea $\mathfrak{p}_i = (X_{m_i}, \cdots, X_{m_{i+1}-1})$.
Cada $\mathfrak{p}_i$ es un ideal primo, luego el complemento de la unión es un conjunto multiplicativo saturado. Sea $\Sigma = B \setminus (\cup_i \mathfrak{p}_i)$.
Vamos a ver que el anillo $A := \Sigma^{-1}A$ es noetheriano.
(1). Primero identificamos los ideales maximales de A. Sea $\mathfrak{m}$ un ideal maximal de A, entonces $\mathfrak{m} = \Sigma^{-1}\mathfrak{n}$ para algún ideal primo $\mathfrak{n}$ tal que $\mathfrak{n} \cap \Sigma = \varnothing$ y $\mathfrak{n}$ es maximal verificando esta condición. En consecuencia $\mathfrak{n} \subseteq \cup_i \mathfrak{p}_i$. Dado $0 \neq x \in \mathfrak{n}$, x se escribe como polinomios en los X_j con un número finito de indeterminadas, y por tanto $x \notin \mathfrak{p}_i$ para i mayor que un cierto entero positivo, esto es, x pertenece sólo a un número finito de ideales $\mathfrak{p}_i$.
Supongamos que $\mathfrak{n}$ es finitamente generado, entre todos los generadores involucran un número finito de indeterminadas, sean $X_1, \ldots, X_s$, llamamos $T = K[X_1, \ldots, X_s]$ y consideramos $\mathfrak{n} \cap T$. Casi todos las intersecciones $\mathfrak{p}_i \cap T$ son cero, y además se verifica $\mathfrak{n} \cap T \subseteq \cup_i(\mathfrak{p}_i \cap T)$. Aplicando la Proposición (4.14.)

existe un índice i tal que $\mathfrak{n}\cap T \subseteq \mathfrak{p}_i \cap T$. En consecuencia $\mathfrak{n}\subseteq \mathfrak{p}_i$, ya que éste último contiene a todos los generadores de $\mathfrak{n}$.

Supongamos ahora que $\mathfrak{n}$ no es finitamente generado. Dado un sistema de generadores de $\mathfrak{n}$, no nulos, $\{n_1, n_2, \ldots\}$, definimos para cada entero positivo j el ideal finitamente generado $\mathfrak{n}_j := (n_1, n_2, \ldots, n_j)$. Para cada uno de estos ideales existe un índice $i(j)$ tal que $\mathfrak{n}_j \subseteq \mathfrak{p}_{i(j)}$. Consideramos ahora el conjunto de estos índice $\{i(j) \mid j \geq 1\}$. Este conjunto es finito, ya que $n_1 \neq 0$ pertenece a todos los $\mathfrak{p}_{i(j)}$, pero n_1 sólo puede pertenecer a un conjunto finito de éstos. Luego si el conjunto C es finito, resulta que $\mathfrak{n}$ está contenido en una unión finita de los $\mathfrak{p}_i$, y aplicando nuevamente la Proposición (4.14.), existe un ideal $\mathfrak{p}_i$ que contiene a $\mathfrak{n}$. En consecuencia $\mathfrak{n}$ es uno de los $\mathfrak{p}_i$ y se tiene $\mathfrak{m} = \Sigma^{-1}\mathfrak{p}_i$.

(2). Para cada ideal maximal $\mathfrak{m}$ de A el localizado $A_{\mathfrak{m}}$ es noetheriano. El ideal $\mathfrak{m}$ corresponde a un ideal primo de B, sea $\mathfrak{n}$. El localizado $A_{\mathfrak{m}}$ se realiza como $\Sigma^{-1}B_{\Sigma^{-1}\mathfrak{n}}$, y por lo tanto es isomorfo a $B_{\mathfrak{n}}$. Para ver que $B_{\mathfrak{n}}$ es noetheriano suponemos que $\mathfrak{n} = \mathfrak{p}_1 = (X_{m_1}, \ldots, X_{m_2-1})$; el cálculo de $B_{\mathfrak{p}_1}$ podemos realizarlo como:

$$B_{\mathfrak{p}_1} = (K[X_{m_2}, X_{m_2+1}, \ldots][X_{m_1}, \ldots, X_{m_2-1}])_{\mathfrak{p}_1} = K(X_{m_2}, X_{m_2+1}, \ldots)[X_{m_1}, \ldots, X_{m_2-1}]_{\mathfrak{p}'_1},$$

que es el localizado de un anillo de polinomios con coeficientes en un cuerpo, y por lo tanto es noetheriano.

(3). El siguiente resultado que necesitamos es comprobar que para cada elemento $0 \neq a \in A$ pertenece solo a un número finito de ideales maximales. Esto es consecuencia del razonamiento en (1).

(4). Veamos que cada ideal de A es finitamente generado. Dado un ideal $\mathfrak{a}$ de A, éste está contenido solo en un número finito de ideales maximales, sean $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ todos los ideales maximales que contienen a $\mathfrak{a}$. Podemos encontrar un conjunto finito de elementos $a_1, \ldots, a_t$ en $\mathfrak{a}$ tales que no existe ningún ideal maximal, distinto de los anteriores que contiene a todos ellos. Utilizando que $A_{\mathfrak{m}_j}$ es noetheriano, existe un número finito de elementos $a_{j,1}, \ldots, a_{j,t_j}$ que generan el ideal $\mathfrak{a}A_{\mathfrak{m}_i}$. Consideramos ahora el conjunto finito

$$C = \{a_1, \ldots, a_t\} \cup \bigcup_j \{a_{j,1}, \ldots, a_{j,t_j}\}.$$

Vamos a ver que $\mathfrak{a} = \sum_{c\in C} aA$.

Para $\mathfrak{m} \neq \mathfrak{m}_j$, $j = 1, \ldots, s$, se tiene:

$$\begin{array}{l} \mathfrak{a}A_{\mathfrak{m}} = A_{\mathfrak{m}}, \text{ ya que } \mathfrak{a} \nsubseteq \mathfrak{m}. \\ \exists a_i, i \in \{1, \ldots, t\}, \text{ tal que } a_i \notin \mathfrak{m}, \text{ entonces } \sum_{c\in C} cA_m = A_{\mathfrak{m}}. \end{array}$$

Para $\mathfrak{m} = \mathfrak{m}_j$, $j \in \{1, \ldots, s\}$, se tiene

$$\mathfrak{a}A_{\mathfrak{m}_j} = (a_{j,1}, \ldots, a_{j,t_j})A_{\mathfrak{m}_j} \subseteq \sum_{c\in C} cA_{\mathfrak{m}_j} \subseteq \mathfrak{a}A_{\mathfrak{m}_j}.$$

Por tanto $\sum_{c\in C} cA_{\mathfrak{m}} = \mathfrak{a}A_{\mathfrak{m}}$ para cada ideal maximal $\mathfrak{m}$, y por tanto se tiene que $\mathfrak{a} = \sum_{c\in C} cA$ es un ideal finitamente generado y A es un anillo noetheriano.

Si identificamos $\mathfrak{p}_i$ con su extendido en A, observa que el anillo $A_{\mathfrak{p}_i}$ tiene dimensión $m_{i+1} - m_i$, por lo tanto el ideal primo $\mathfrak{p}_i$ tiene altura $m_{i+1} - m_i$. Como estos números van creciendo se tiene que la dimensión de A es infinita.

47. Ejercicios

Anillos noetherianos

Anillos artinianos

Ejercicio. 47.1.
Prueba que todo módulo artiniano sobre un anillo artiniano es un módulo noetheriano.

SOLUCIÓN

Ejercicio. 47.2.
Sea K un cuerpo y $A = \frac{K[X^2,X^3]}{(X^4)} \subseteq \frac{K[X]}{(X^4)}$.
(1) Prueba que A es un anillo artiniano.
(2) Prueba que A es un anillo local con ideal maximal $\mathfrak{m} = (X^2, X^3)$.
(3) Determina el nilradical de A.

SOLUCIÓN

Dimensión de anillos

Ejercicio. 47.3.
Demuestra que para cada anillo A se tiene:

$$\dim(A) = \sup\{\dim(A_\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(A)\}.$$

SOLUCIÓN

Ejercicio. 47.4.
Demuestra que si $\mathfrak{a}$ es un ideal nilpotente de un anillo A, entonces:

$$\dim(A) = \dim(A/\mathfrak{a}).$$

SOLUCIÓN

Ejercicio. 47.5.
Sea K un cuerpo y $\mathfrak{a} \subseteq K[X_1, \ldots, X_n]$ el ideal generado por los siguientes polinomios de grado uno:

$$\mathfrak{a} = \begin{pmatrix} F_1 = \sum_{i=0}^n a_{1,i}X_i, \\ \vdots \\ F_s = \sum_{i=0}^n a_{s,i}X_i \end{pmatrix}$$

Si r es el rango del sistema de ecuaciones lineales:

$$\left.\begin{array}{c} \sum_{i=1}^n a_{1,i}X_i = a_{1,0} \\ \vdots \\ \sum_{i=1}^n a_{s,i}X_i = a_{s,0} \end{array}\right\}$$

Prueba que la dimensión del anillo $K[X_1, \ldots, X_n]/\mathfrak{a}$ es igual a $n - r$.

SOLUCIÓN

Ejercicio. 47.6.
Sea K un cuerpo. Prueba que toda K–álgebra afín (cociente de un anillo de polinomios en un número finito de indeterminadas) tiene dimensión cero (es artiniano) si y solo si es finito dimensional sobre K.

SOLUCIÓN

Ejercicio. 47.7.
Calcula la dimensión del anillo $\mathbb{Z}[X,Y]/(X^2 + Y^2 - 1, XY - Y^2X + 3)$.

SOLUCIÓN

Ejercicio. 47.8.
Calcula la altura de los siguientes ideales:

(1) $\mathfrak{a} = (X, Y - 1) \subseteq K[X,Y]$.
(2) $\mathfrak{b} = (X + Y, X - Y) \subseteq K[X,Y]$.

SOLUCIÓN

Ejercicio. 47.9.
Prueba que para cualesquiera ideales $\mathfrak{a}, \mathfrak{b}$ *de un anillo* A *son equivalentes:*

(1) $\operatorname{rad}(\mathfrak{a}) = \operatorname{rad}(\mathfrak{b})$.
(2) $\mathfrak{a}$ *y* $\mathfrak{b}$ *tienen los mismos ideales primos minimales.*

SOLUCIÓN

Ejercicio. 47.10.
Sea K *un cuerpo.Dado el ideal* $\mathfrak{a} = (X^2 - XY + X, XY - Y^2 + Y) \subseteq K[X, Y]$, *calcula la dimensión de* $K[X, Y]/\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 47.11.
Prueba los siguientes enunciados

(1) Si D *es un dominio de integridad de dimensión cero, entonces* D *es un cuerpo.*
(2) Si D *es un DIP que no es un cuerpo, prueba que la dimensión de* D *es igual a uno.*
(3) Si $\mathfrak{a} \subseteq A$ *es un ideal, entonces* $\mathfrak{a}[X] = \mathfrak{a}A[X]$.
(4) Si $\dim(A) = \infty$, *entonces* $\dim(A[X]) = \infty$.

SOLUCIÓN

Ejercicio. 47.12. (Teorema de Seidenberg)
Sea A *un anillo de dimensión finita* n. *Prueba que*

$$n + 1 \leq \dim(A[X]) \leq 2n + 1.$$

Nota: Cuando A *es un anillo noetheriano se tiene* $\dim(A[X]) = \dim(A) + 1$; *para la demostración necesitamos el Teorema del ideal principal.*

SOLUCIÓN

Ejercicios del capítulo

Ejercicio. 47.13.
Responde a las cuestiones o prueba la verdad o falsedad, según el caso, de las siguientes afirmaciones:

(1) *En un anillo (conmutativo) artiniano todo ideal primo es maximal.*
(2) *¿Es cierto el recíproco?*
(3) *¿Cómo son los dominios de integridad artinianos?*
(4) *Da un ejemplo de un anillo artiniano local que no sea un D.I.*
(5) *Si un anillo A verifica que todo cociente $A/\mathfrak{a}$ es artiniano, para $\mathfrak{a} \neq 0$, ¿es A artiniano?*
(6) *Si A es un anillo local artiniano, ¿forman los ideales de A una cadena?*
(7) *Si K es un cuerpo, ¿es toda K–álgebra de K–dimensión finita artiniana?*
(8) *Si K es un cuerpo, ¿es toda K–álgebra A, con $\dim(A) < \infty$, artiniana?*
(9) *En un anillo artiniano todo elemento regular (no divisor de cero) es invertible.*
(10) *Si en un anillo noetheriano A todo elemento regular es invertible, entonces A es artiniano.*

SOLUCIÓN

Capítulo IX

Descomposición primaria

Introducción

El estudio de los conjuntos algebraicos se reduce a encontrar descomposiciones de los mismos en términos de sus componentes irreducibles. Desde el punto de vista algebraico se trata de dar una descomposición del ideal como una intersección de ciertos ideales: los ideales primarios. El objetivo del capítulo es probar que cada ideal en un anillo noetheriano tiene una descomposición primaria: posteriormente esta descomposición se prueba también para módulos noetherianos. Se aplica esta teoría en algunos caso concretos, centrándonos en dos: la clasificación de los conjuntos algebraicos del plano y la descomposición en los anillos de polinomios.

48. Descomposición primaria de ideales

Ideales primarios

Un ideal $\mathfrak{q}$ de un anillo conmutativo A se llama **primario** si (i) es propio, y (ii) verifica la siguiente condición: para elementos $a, b \in A$ tales que $ab \in \mathfrak{q}$, y $a \notin \mathfrak{q}$, existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{q}$.

Lema. 48.1.
Sea A un anillo conmutativo y $\mathfrak{q}$ un ideal propio de A. Son equivalentes los siguientes enunciados:
(a) $\mathfrak{q}$ es un ideal primario;
(b) Cada divisor de cero en $A/\mathfrak{q}$ es un elemento nilpotente.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Sea $x+\mathfrak{q} \in A/\mathfrak{q}$ un divisor de cero, entonces existe $0 \neq y+\mathfrak{q}$ tal que $0=(x+\mathfrak{q})(y+\mathfrak{q})=xy+\mathfrak{q}$ y tenemos $xy \in \mathfrak{q}$, como $y \notin \mathfrak{q}$, entonces existe $n \in \mathbb{N}$ tal que $x^n \in \mathfrak{q}$ y $x+\mathfrak{q}$ es nilpotente.
(b) $\Rightarrow$ (a). Sea $xy \in \mathfrak{q}$, $y \notin \mathfrak{q}$, entonces $0=(x+\mathfrak{q})(y+\mathfrak{q})$ y $y+\mathfrak{q} \neq 0$, luego $x+\mathfrak{q}$ es un divisor de cero y es nilpotente, esto es, existe $n \in \mathbb{N}$ tal que $(x+\mathfrak{q})^n=0$, entonces $x^n \in \mathfrak{q}$ y $\mathfrak{q}$ es primario. □

Lema. 48.2.
Si $\mathfrak{q}$ es un ideal primario de un anillo conmutativo A, entonces $\operatorname{rad}(\mathfrak{q})$ es un ideal primo.

DEMOSTRACIÓN. Sea $xy \in \operatorname{rad}(\mathfrak{q})$, si $x \notin \operatorname{rad}(\mathfrak{q})$, entonces para cada $n \in \mathbb{N}$ se tiene $x^n \notin \mathfrak{q}$. Como consecuencia $y \in \mathfrak{q} \subseteq \operatorname{rad}(\mathfrak{q})$. □

Si $\mathfrak{q}$ es primario y $\operatorname{rad}(\mathfrak{q})=\mathfrak{p}$, entonces decimos que $\mathfrak{q}$ es un **ideal $\mathfrak{p}$–primario**.

Ejemplo. 48.3.
En el anillo $\mathbb{Z}$ de los números enteros los ideales primarios son de la forma $p^n\mathbb{Z}$, para p un número entero primo y $n \in \mathbb{N}$.

Sin embargo, si el anillo no es un DIP, un ideal primario no ha de ser necesariamente una potencia de un ideal primo.

Ejemplo. 48.4.
Sea $A=K[X,Y]$ el anillo de polinomios con coeficientes en un cuerpo y $\mathfrak{q}=(X,Y^2)$. Es claro que $\mathfrak{q}$ es primario, pues $A/\mathfrak{q} \cong K[Y]/(Y^2)$ verifica que cada divisor de cero es nilpotente. Sin embargo, el radical de (X,Y^2) es (X,Y) y se verifica: $(X,Y)^2 \subseteq (X,Y^2) \subseteq (X,Y)$.
Observa que $(X,Y)^2$ es un ideal primario, ya que si $FG \in (X,Y)^2$ y $F \notin (X,Y)^2 \subseteq (X,Y)$, si $G \notin (X,Y)$, entonces $(X,Y)+(G)=K[X,Y]$, lo que implica que existen $H \in (X,Y)^2$ y $L \in K[X,Y]$ tales que $H+LG=1$, entonces $F=FH+LFG \in (X,Y)^2$, lo que es una contradicción.

El siguiente ejemplo prueba que no es tampoco suficiente para que un ideal sea primario el que sea la potencia de un ideal primo, ni que su radical sea primo.

Ejemplo. 48.5.
Sea $A = K[X, Y, Z]/(XY - Z^2)$, llamamos x, y, z a las clases de X, Y, Z, respectivamente, en A. Tenemos que el ideal $\mathfrak{p} = (x, z)$ es un ideal primo, y que $\mathfrak{p}^2$ no es un ideal primario, ya que $xy = z^2 \in \mathfrak{p}^2$, y se tiene que $x \notin \mathfrak{p}^2$ e $y^n \notin \mathfrak{p}^n$ para todo $n \in \mathbb{N}$.

Por el contrario, toda potencia de un ideal maximal siempre es un ideal primario.

Lema. 48.6.
Sea A un anillo conmutativo y $\mathfrak{q}$ un ideal propio. Si $\operatorname{rad}(\mathfrak{q})$ es un ideal maximal, entonces $\mathfrak{q}$ es un ideal primario. En particular las potencias de un ideal maximal son ideales primarios.

DEMOSTRACIÓN. Se considera el cociente $A/\mathfrak{q}$, como $\operatorname{rad}(\mathfrak{q}) = \mathfrak{m}$ es un ideal maximal, resulta que $A/\mathfrak{q}$ tiene un único ideal primo, luego cada divisor de cero es nilpotente y $\mathfrak{q}$ es un ideal primario. □

Corolario. 48.7.
Sea A un anillo conmutativo, $\mathfrak{m} \subseteq A$ un ideal maximal y $\mathfrak{q}$ un ideal tal que $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algún $n \in \mathbb{N}$, entonces $\mathfrak{q}$ es un ideal $\mathfrak{m}$–primario.

DEMOSTRACIÓN. Es claro, ya que $\operatorname{rad}(\mathfrak{q}) = \mathfrak{m}$. □

Descomposición primaria de ideales

Lema. 48.8.
Sea A un anillo conmutativo y $\{\mathfrak{q}_\alpha \mid \alpha \in \Lambda\}$ una familia finita de ideales $\mathfrak{p}$–primarios, entonces $\cap_\alpha \mathfrak{q}_\alpha$ es un ideal $\mathfrak{p}$–primario.

DEMOSTRACIÓN. Se tiene $\operatorname{rad}(\cap_\alpha \mathfrak{q}_\alpha) = \cap_\alpha \operatorname{rad}(\mathfrak{q}_\alpha) = \mathfrak{p}$. Por otro lado, si $xy \in \cap_\alpha \mathfrak{q}_\alpha$ y $x \notin \cap_\alpha \mathfrak{q}_\alpha$, entonces existe un índice β tal que $x \notin \mathfrak{q}_\beta$, luego existe $n \in \mathbb{N}$ tal que $y^n \in \mathfrak{q}_\beta$ y por tanto $y \in \mathfrak{p}$. Entonces existe $m \in \mathbb{N}$ tal que $y^m \in \cap_\alpha \mathfrak{q}_\alpha$. □

Proposición. 48.9.
Sea A un anillo conmutativo y $\mathfrak{q}$ un ideal $\mathfrak{p}$–primario. Para cada $x \in A$ se verifica:
(1) $x \in \mathfrak{q}$ si, y sólo si, $(\mathfrak{q} : x) = A$;
(2) $x \notin \mathfrak{q}$ si, y sólo si, $(\mathfrak{q} : x)$ es $\mathfrak{p}$–primario;
(3) $x \notin \mathfrak{p}$ si, y sólo si, $(\mathfrak{q} : x) = \mathfrak{q}$.

DEMOSTRACIÓN. (1). Es consecuencia directa de la definición.
(2). Si $x \notin \mathfrak{q}$ y $ab \in (\mathfrak{q} : x)$ con $a \notin (\mathfrak{q} : x)$, entonces $abx \in$ y $ax \notin \mathfrak{q}$, luego existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{q}$, en particular $b^n \in (\mathfrak{q} : x)$, luego $(\mathfrak{q} : x)$ es primario. El recíproco es inmediato, ya que cada ideal primario es un ideal propio.
Para ver que es $\mathfrak{p}$–primario, comprobamos la igualdades siguientes:

$$\begin{aligned} \operatorname{rad}(\mathfrak{q} : x) &= \{a \mid \exists n \in \mathbb{N},\ a^n \in (\mathfrak{q} : x)\} = \{a \mid \exists n \in \mathbb{N},\ a^n x \in \mathfrak{q}\} \\ &= \{a \mid \exists n \in \mathbb{N},\ a^n \in \mathfrak{q}\} \qquad = \operatorname{rad}(\mathfrak{q}) = \mathfrak{p}. \end{aligned}$$

(3). Es consecuencia directa de la definición. □

Si $\mathfrak{a}$ es un ideal propio de A, una **descomposición primaria** de $\mathfrak{a}$ es una expresión del tipo:

$$\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i,$$

con $\mathfrak{q}_i$ ideales primarios. Una descomposición primaria se llama **reducida** si verifica las dos condiciones siguientes:

(I) $\operatorname{rad}(\mathfrak{q}_i) \neq \operatorname{rad}(\mathfrak{q}_j)$ si $i \neq j$;
(II) $\mathfrak{q}_i \not\supseteq \cap_{j\neq i}\mathfrak{q}_j$ para cada índice $i = 1, \ldots, n$.

Un ideal $\mathfrak{a}$ se llama **descomponible** si tiene una descomposición primaria.

Ejemplo. 48.10.
Dado un ideal $n\mathbb{Z} \subseteq \mathbb{Z}$, si la factorización en elementos primos de n es: $n = p_1^{e_1} \cdots p_t^{e_t}$, se tiene cada $(p_i\mathbb{Z})^{e_i}$ es un ideal $p_i\mathbb{Z}$–primario y que $n\mathbb{Z} = (p_1\mathbb{Z})^{e_1} \cdots (p_t\mathbb{Z})^{e_t} = (p_1\mathbb{Z})^{e_1} \cap \ldots \cap (p_t\mathbb{Z})^{e_t}$ es una descomposición primaria reducida de $n\mathbb{Z}$.

Lema. 48.11.
Todo ideal descomponible tiene una descomposición primaria reducida.

DEMOSTRACIÓN. Es consecuencia del Lema (48.8.). □

Teorema. 48.12. (Primer teorema de unicidad.)
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal con una descomposición primaria reducida $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$. Sea $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ para cada índice i. Entonces los ideales $\mathfrak{p}_i$ son todos los ideales primos que se pueden escribir en la forma $\operatorname{rad}(\mathfrak{a}\colon x)$, para $x \in A$.
Como consecuencia son independientes de la elección de la descomposición primaria considerada.

DEMOSTRACIÓN. Dado $x \in A$ tenemos $(\mathfrak{a} : x) = (\cap_i \mathfrak{q}_i : x) = \cap_i(\mathfrak{q}_i : x)$, luego $\operatorname{rad}(\mathfrak{a} : x) = \operatorname{rad}(\cap_i(\mathfrak{q}_i : x)) = \cap_i \operatorname{rad}(\mathfrak{q}_i : x) = \cap\{\mathfrak{p}_i \mid\ x \notin \mathfrak{q}_i,\ i = 1, \ldots, n\}$. Para cada uno de los $\mathfrak{p}_i$, tomando $x \in \cap_{j\neq i}\mathfrak{q}_j \setminus \mathfrak{q}_i$, y tenemos $\operatorname{rad}(\mathfrak{a} : x) = \operatorname{rad}(\mathfrak{q}_i : x) = \mathfrak{p}_i$.
Por otro lado, para un ideal primo cualquiera $\mathfrak{p}$, si $\mathfrak{a} : x$ es $\mathfrak{p}$–primario, entonces $\mathfrak{p} = \operatorname{rad}(\mathfrak{a}_x) = \cap_{x\notin\mathfrak{q}_j}\mathfrak{q}_j = \cap_j \mathfrak{p}_j$, luego existe un índice j tal que $\mathfrak{p} = \mathfrak{p}_j$. □

Corolario. 48.13.
En la situación anterior, para cada índice i existe un elemento $x_i \in A$ tal que $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{a} : x_i)$ y $(\mathfrak{a} : x_i)$ es primario.

Los ideales $\mathfrak{p}_i$ se llaman **divisores primos** del ideal $\mathfrak{a}$.
El conjunto de los divisores primos del ideal $\mathfrak{a}$ se representa por $\operatorname{Ass}_{dp}(A/\mathfrak{a})$ o por $\operatorname{Ass}(A/\mathfrak{a})$.

Proposición. 48.14.
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal con una descomposición primaria reducida. Para cada ideal primo $\mathfrak{p}$ tal que $\mathfrak{p} \supseteq \mathfrak{a}$, existe un ideal primo minimal $\mathfrak{q}$ verificando $\mathfrak{p} \supseteq \mathfrak{q} \supseteq \mathfrak{a}$.
Además los ideales primos minimales sobre $\mathfrak{a}$ son exactamente los elementos minimales de $\operatorname{Ass}_{dp}(A/\mathfrak{a})$.

DEMOSTRACIÓN. La primera parte es consecuencia del Lema de Zorn. Para la segunda, si $\mathfrak{p} \supseteq \mathfrak{a}$ es minimal sobre $\mathfrak{a}$, de $\mathfrak{p} \supseteq = \mathfrak{a} = \cap_i \mathfrak{q}_i$ tenemos que existe un índice i tal que $\mathfrak{p} \supseteq \mathfrak{p}_i \supseteq \mathfrak{a}$, y por la minimalidad se tiene $\mathfrak{p} = \mathfrak{p}_i$. □

Proposición. 48.15.
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal con una descomposición primaria reducida $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$. Sea $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ para cada índice i. Entonces

$$\cup_{i=1}^n \mathfrak{p}_i = \{x \in A \mid\ (\mathfrak{a}\colon x) \neq \mathfrak{a}\}.$$

En particular si 0 *es un ideal con descomposición primaria, entonces el conjunto de los divisores de cero de* A *es la unión de los divisores primos del ideal* 0.

DEMOSTRACIÓN. Podemos considerar que $\mathfrak{a} = 0$ pasando al cociente $A/\mathfrak{a}$. Vamos entonces a ver que el conjunto D de los divisores de cero de A es la unión de los divisores primos de A. Es claro que $D \subseteq \cup\mathfrak{p}_i$ ya que tenemos $D = \cup_x(0 : x) = \cup_x \operatorname{rad}(0 : x)$, y $\operatorname{rad}(0 : x) = \cap_{x\notin\mathfrak{q}_j} \operatorname{rad}(\mathfrak{q}_j) \subseteq \mathfrak{p}_j \in \operatorname{Ass}_{dp}(A)$. Recíprocamente, como cada $\mathfrak{p}_i$ es de la forma $\operatorname{rad}(0 : x_i)$ para algún $x_i \in A$, entonces $\mathfrak{p}_i \subseteq D$ y tenemos la igualdad. □

Proposición. 48.16.
Sea A *un anillo conmutativo y* Σ *un subconjunto multiplicativo. Si* $\mathfrak{q}$ *es un ideal* $\mathfrak{p}$*–primario de* A *se verifica:*

(1) Si $\Sigma \cap \mathfrak{p} \neq \varnothing$*, entonces* $\Sigma^{-1}\mathfrak{q} = \Sigma^{-1}A$*;*
(2) Si $\Sigma \cap \mathfrak{p} = \varnothing$*, entonces* $\Sigma^{-1}\mathfrak{q}$ *es* $\Sigma^{-1}\mathfrak{p}$*–primario y* $\mathfrak{q} = \mathfrak{q}^{ec}$*.*

Como consecuencia, existe una correspondencia biyectiva entre ideales primarios de $\Sigma^{-1}A$ *y los ideales primarios que no cortan a* Σ*.*

DEMOSTRACIÓN. Si $\Sigma \cap \mathfrak{p} \neq \varnothing$, entonces existe $s \in \Sigma \cap \mathfrak{p}$, como $\mathfrak{p} = \operatorname{rad}(\mathfrak{q})$, existe $n \in \mathbb{N}$ tal que $s^n \in \mathfrak{q}$, luego $\Sigma^{-1}\mathfrak{q} = \Sigma^{-1}A$.
Si $\Sigma \cap \mathfrak{p} = \varnothing$, vamos a probar que $\Sigma^{-1}\mathfrak{q}$ es primario. Sea $(a/1)(b/1) \in \Sigma^{-1}\mathfrak{q}$, $a/1 \notin \Sigma^{-1}\mathfrak{q}$, entonces existe $s \in \Sigma$ tal que $abs \in \mathfrak{q}$ y $as \notin \mathfrak{q}$. Luego existe $n \in \mathbb{N}$ tal que $b^n \in \mathfrak{q}$, en consecuencia $b/1 \in \Sigma^{-1}\mathfrak{p}$.
Ahora comprobamos que es $\Sigma^{-1}\mathfrak{p}$–primario; $\operatorname{rad}(\Sigma^{-1}\mathfrak{q}) = \Sigma^{-1}\operatorname{rad}(\mathfrak{q}) = \Sigma^{-1}\mathfrak{p}$. Falta ver que $\mathfrak{q}^{ec} \subseteq \mathfrak{q}$; dado $x \notin \mathfrak{q}^{ec} \setminus \mathfrak{q}$, se tiene $x/1 \in \Sigma^{-1}\mathfrak{q}$, luego existe $s \in \Sigma$ tal que $sx \in \mathfrak{q}$, y como $x \notin \mathfrak{q}$, existe $n \in \ltimes$ tal que $s^{\in}\mathfrak{q}$, esto es, $s \in \mathfrak{p} \cap \Sigma = \varnothing$, lo que es una contradicción. □

Para cada ideal $\mathfrak{a}$ de un anillo A y cada subconjunto multiplicativo Σ, llamamos $\operatorname{Sat}_\Sigma(\mathfrak{a})$ a la Σ–**saturación** de $\mathfrak{a}$, esto es, a $\operatorname{Sat}_\Sigma(\mathfrak{a}) = (\Sigma^{-1}\mathfrak{a})^c = \mathfrak{a}^{ec}$.

Proposición. 48.17.
Sea A *un anillo conmutativo,* Σ *un subconjunto multiplicativo y* $\mathfrak{a}$ *un ideal de* A *con una descomposición primaria reducida* $\mathfrak{a} = \cap_{i=1}^n\mathfrak{q}_i$*. Sea* $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$ *para cada índice* i*. Supongamos que* $\mathfrak{p}_j \cap \Sigma = \varnothing$ *para* $j = 1, \ldots, m$ *y* $\mathfrak{p}_j \cap \Sigma \neq \varnothing$ *para* $j = m + 1, \ldots, n$*. Entonces*

$$\Sigma^{-1}\mathfrak{a} = \cap_{i=1}^m\Sigma^{-1}\mathfrak{q} \qquad y \qquad \operatorname{Sat}_\Sigma(\mathfrak{a}) = \cap_{i=1}^m\mathfrak{q}_i$$

son descomposiciones primarias reducidas.

Un subconjunto $\mathcal{P}$ de $\operatorname{Spec}(A)$ se llama **genéricamente estable** cuando verifica que:

$$\text{si } \mathfrak{p} \in \mathcal{P} \text{ y } \mathfrak{p}' \subseteq \mathfrak{p}, \text{ entonces } \mathfrak{p}' \in \mathcal{P}.$$

Ejemplo. 48.18.
Dado un conjunto multiplicativo $\Sigma \subseteq A$ el conjunto $\mathcal{P} = \{\mathfrak{p} \mid \mathfrak{p} \cap \Sigma = \varnothing\}$ es un conjunto genéricamente estable.

Teorema. 48.19. (Segundo teorema de unicidad.)
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal con una descomposición primaria reducida $\mathfrak{a} = \cap_{i=1}^n \mathfrak{q}_i$. Sea $\operatorname{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, para cada índice i. Si $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ es un conjunto genéricamente estable contenido en $\operatorname{Ass}_{dp}(A/\mathfrak{a})$, entonces $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ es independiente de la descomposición primaria.

Observa que el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ puede estar propiamente contenido en $\operatorname{Ass}_{dp}(A/\mathfrak{a})$.

DEMOSTRACIÓN. Llamamos $\Sigma = A \setminus (\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_m)$, entonces Σ es un conjunto multiplicativamente cerrado. Para cada ideal primo $\mathfrak{p}$, divisor primo de $\mathfrak{a}$, se tiene $\mathfrak{p} \cap \Sigma = \varnothing$, si $\mathfrak{p} \in \{\mathfrak{p}_1 \ldots, \mathfrak{p}_m\}$, ó $\mathfrak{p} \cap \Sigma \neq \varnothing$, si $\mathfrak{p} \notin \{\mathfrak{p}_1 \ldots, \mathfrak{p}_m\}$. Entonces $\Sigma^{-1}\mathfrak{a} = \Sigma^{-1}\mathfrak{q}_1 \cap \ldots \cap \Sigma^{-1}\mathfrak{q}_m$, y se tiene $\operatorname{Sat}_\Sigma(\mathfrak{a}) = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m$. □

Si $\mathfrak{a}$ es un ideal con una descomposición primaria, cada elemento minimal de $\operatorname{Ass}_{dp}(A/\mathfrak{a})$ se llama un divisor primo **aislado**, los restantes divisores primos se llaman **embebidos**.
Si $\mathfrak{p}_i$ es un divisor primo aislado, entonces $\mathfrak{q}_i$ se llama **componente primaria aislada**, las otras se llaman **componentes primarias embebidas**.
Observa que cualquier conjunto de divisores primos aislados es un subconjunto genéricamente estable.

Corolario. 48.20.
Sea A un anillo conmutativo y $\mathfrak{a}$ un ideal con una descomposición primaria. Las componentes primarias aisladas están determinadas de forma única.

Por el contrario las componentes embebidas no están determinadas de forma única como el siguiente ejemplo muestra.

Ejemplo. 48.21.
Se considera el anillo $A = K[X, Y]$ y el ideal $\mathfrak{a} = (X^2, XY)$. Llamamos $\mathfrak{p}_1 = (X)$ y $\mathfrak{p}_2 = (X, Y)$. Entonces $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$ es una descomposición primaria de A. Entonces como $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$, entonces $\mathfrak{p}_1$ es un primo aislado y $\mathfrak{p}_2$ es un primo embebido.
Otra descomposición primaria de $\mathfrak{a}$ es $\mathfrak{a} = (X) \cap (X^2, Y)$. En este caso la componente aislada es (X) y la componente embebida es (X^2, Y), lo que prueba que las componentes embebidas no están determinadas de forma única.

49. Conjuntos algebraicos irreducibles

Un conjunto algebraico afín V se llama **irreducible** si cuando $V = V_1 \cup V_2$, para V_1, V_2 conjuntos algebraicos afines, se verifica $V = V_1$ o $V = V_2$.

Esta definición puede también extenderse a subconjuntos arbitrarios de $\mathbb{A}^n$. Un subconjunto $X \subseteq \mathbb{A}^n$ es **irreducible** si cuando $X = X_1 \cup X_2$, para $X_1, X_2 \subseteq X$ cerrados, se verifica $X = X_1$ ó $X = X_2$.

Proposición. 49.1.
Un conjunto algebraico afín V es irreducible si, y sólo si, $\mathcal{I}(V)$ es un ideal primo.

DEMOSTRACIÓN. ($\Rightarrow$). Si $\mathfrak{a}_1$, $\mathfrak{a}_2$ son ideales de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$ tales que $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathcal{I}(V)$, podemos suponer que $\mathcal{I}(V) \subseteq \mathfrak{a}_i$ y tenemos:

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathcal{I}(V) \Rightarrow V = \mathcal{V}\mathcal{I}(V) \subseteq \mathcal{V}(\mathfrak{a}_1\mathfrak{a}_2) = \mathcal{V}(\mathfrak{a}_1) \cup \mathcal{V}(\mathfrak{a}_2);$$

$$\mathcal{I}(V) \subseteq \mathfrak{a}_i \Rightarrow \mathcal{V}(\mathfrak{a}_i) \subseteq \mathcal{V}\mathcal{I}(V) = V.$$

Y se verifica:

$$V = \mathcal{V}(\mathfrak{a}_1) \cup \mathcal{V}(\mathfrak{a}_2) \Rightarrow \begin{cases} V = \mathcal{V}(\mathfrak{a}_1) \Rightarrow \mathcal{I}(V) = \mathcal{I}\mathcal{V}(\mathfrak{a}_1) \supseteq \mathfrak{a}_1 \\ \text{o} \\ V = \mathcal{V}(\mathfrak{a}_2) \Rightarrow \mathcal{I}(V) = \mathcal{I}\mathcal{V}(\mathfrak{a}_2) \supseteq \mathfrak{a}_2 \end{cases}$$

($\Leftarrow$). Sea $V = V_1 \cup V_2$, entonces se verifica:

$$\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2) \supseteq \mathcal{I}(V_1)\mathcal{I}(V_2).$$

Y por tanto

$$\begin{cases} \mathcal{I}(V_1) \supseteq \mathcal{I}(V) \Rightarrow V_1 = \mathcal{V}\mathcal{I}(V_1) \supseteq \mathcal{V}\mathcal{I}(V) = V; \\ \text{o} \\ V_2 = \mathcal{V}\mathcal{I}(V_2) \supseteq \mathcal{V}\mathcal{I}(V) = V. \end{cases}$$

□

Veamos el caso particular de una hipersuperficie sobre un cuerpo algebraicamente cerrado.

Lema. 49.2.
Sea K es algebraicamente cerrado y $n \geq 1$. Si $F \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$ es un polinomio no constante y $F = uF_1^{e_1} \cdots F_r^{e_r}$, es la factorización en irreducibles de F en $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$, entonces $\mathcal{I}\mathcal{V}(F) = (F_1 \cdots F_r)$.

Corolario. 49.3.
Sea K un cuerpo algebraicamente cerrado y $n \geq 1$. Una hipersuperficie $\mathcal{V}(F)$ es irreducible si, y sólo si, es el conjunto de ceros de un polinomio irreducible.

Corolario. 49.4.
Sea K un cuerpo algebraicamente cerrado y $n \geq 1$. Cada hipersuperficie se puede representar en la forma

$$H = H_1 \cup \cdots \cup H_s, \quad H_i \neq H_j \text{ si } i \neq j \text{ y } H_i \text{ irreducible}$$

Esta representación es única salvo en el orden.

Un resultado de este tipo puede generalizarse a conjuntos algebraicos arbitrarios. Para ello necesitamos el siguiente resultado previo.

Lema. 49.5.
Cada familia no vacía de conjuntos algebraicos afines tiene un elemento minimal o equivalentemente se verifica la condición de cadena descendente para conjuntos algebraicos.

DEMOSTRACIÓN. Sea $\{V_i\}$ una cadena descendente de conjuntos algebraicos. Si llamamos $\mathfrak{a}_i = \mathcal{I}(V_i)$, tenemos una cadena ascendente $\{\mathfrak{a}_i\}$ de ideales de $\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]$. Como este anillo es noetheriano, resulta que existe un índice n tal que $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \ldots$ Como $V_i = \mathcal{V}(\mathfrak{a}_i)$, resulta que $V_n = V_{n+1} = \ldots$, y por tanto se verifica la condición de cadena ascendente. □

Lema. 49.6.
Sea X un conjunto de $\mathbb{A}^n$. Son equivalentes:
(a) X is irreducible;
(b) Para cada par de subconjuntos abiertos no vacíos U_1 y U_2 de X se verifica que $U_1 \cap U_2 \neq \varnothing$;
(c) $\overline{X}$ es irreducible.

DEMOSTRACIÓN. La equivalencia (a) ⇔ (b) es trivial, ya que es únicamente tomar complementario. La equivalencia (b) ⇔ (c) es inmediata usando que X es denso en $\overline{X}$. □

Teorema. 49.7.
Si V es un conjunto algebraico afín en $\mathbb{A}^n$, entonces V es la unión de sus subconjuntos algebraicos irreducible maximales.

DEMOSTRACIÓN. Probamos primero que V es la unión de sus subconjuntos algebraicos irreducibles maximales. Ya que para cada punto $(a_1, \ldots, a_n) \in V$ tenemos que $\{(a_1, \ldots, a_n)\}$ es un subconjunto irreducible, basta ver que cada subconjunto irreducible está contenido en un subconjunto algebraico irreducible maximal.
Sea $Y \subseteq V$ un subconjunto irreducible; definimos

$$\Gamma = \{Z \mid \ Y \subseteq Z \text{ y } Z \text{ es irreducible}\}.$$

Se tiene que Γ es no vacío, pues contiene a Y. Sea ahora una cadena ascendente $\{Z_i\}$ de elementos de Γ. Llamamos $Z = \cup_i Z_i$. Vamos a ver que Z es irreducible. Sean U_1, $U_2 \subseteq \mathbb{A}^n$ subconjuntos abiertos tales que $U_j \cap Z \neq \varnothing$, entonces existen índices i_1, i_2 tales que $U_j \cap Z_{i_j} \neq \varnothing$. Sea h un índice tal que $h \geq i_1, i_2$, entonces $U_j \cap Z_h \neq \varnothing$, y como Z_h es irreducible, resulta que $U_1 \cap U_2 \cap Z_h \neq \varnothing$, esto es, tenemos $U_1 \cap U_2 \cap Z \neq \varnothing$. Entonces Z es irreducible. Aplicando ahora el Lema de Zorn resulta que Γ tiene elementos maximales. Como consecuencia del Lema anterior tenemos además que cada uno de estos elementos maximales es cerrado, y por tanto es un subconjunto algebraico irreducible maximal. □

Cada uno de los subconjuntos algebraicos irreducible maximales que aparecen en el Teorema anterior se llama una **componente irreducible** de V.
Vamos a estudiar ahora la finitud del número de componentes irreducibles.

Teorema. 49.8.
Si V es un conjunto algebraico afín no vacío en $\mathbb{A}^n$, existe un número finito de componentes irreducibles $V_1, \ldots, V_r \subseteq V$, unívocamente determinadas, tales que

$$V = V_1 \cup \cdots \cup V_r,\ V_j \nsubseteq \cup_{i\neq j} V_i \text{ y } V_i \neq V_j \text{ si } i \neq j.$$

DEMOSTRACIÓN. Llamamos Γ al conjunto de todos los conjuntos algebraicos que no son una unión finita de subconjuntos algebraicos irreducibles. Si Γ es no vacío, existe un elemento V minimal en Γ. Como $V \in \Gamma$, resulta que V no es irreducible, entonces existen $V_1, V_2 \subset V$ subconjuntos algebraicos tales que $V = V_1 \cap V_2$. Por la minimalidad de V resulta que $V_i \notin \Gamma$ y por tanto son uniones finitas de subconjuntos algebraicos irreducibles, y en consecuencia V también lo es, lo que es una contradicción. □

La expresión $V = V_1 \cup \cdots \cup V_r$ se llama la **descomposición en componentes irreducibles** de V.

Aplicación de la descomposición primaria a conjuntos algebraicos

Dado un conjunto algebraico $V = \mathcal{V}(\mathfrak{a})$ para $\mathfrak{a}$ un ideal de $K[X_1, \ldots, X_n]$.
Supongamos que $\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t$ es una descomposición primaria minimal de $\mathfrak{a}$, entonces se verifica:

$$V = \mathcal{V}(\mathfrak{a}) = \mathcal{V}(\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_t) = \mathcal{V}(\mathfrak{q}_1) \cup \cdots \cup \mathcal{V}(\mathfrak{q}_t).$$

Cada $\mathfrak{q}_i$ es un ideal primario, supongamos que $\mathrm{rad}(\mathfrak{q}_i) = \mathfrak{p}_i$, entonces $\mathcal{V}(\mathfrak{q}_i) = \mathcal{V}(\mathfrak{p}_i)$, para cada índice i, y por tanto tenemos la siguiente expresión para V:

$$V = \mathcal{V}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{V}(\mathfrak{p}_t).$$

Supongamos que $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son los ideales primos aislados de $\mathfrak{a}$ (los elementos minimales del conjunto $\mathrm{Ass}(\mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}]/\mathfrak{a})$), y que por tanto $\mathfrak{p}_{r+1}, \ldots, \mathfrak{p}_t$ sean los ideales primos embebidos. Entonces para cada $\mathfrak{p}_{r+j}$, $j = 1, \ldots, t-r$, existe un $\mathfrak{p}_i$, $i = 1, \ldots, r$, tal que $\mathfrak{p}_i \subseteq \mathfrak{p}_{r+j}$ y por tanto $\mathcal{V}(\mathfrak{p}_{r+j}) \subseteq \mathcal{V}(\mathfrak{p}_i)$, esto es, $\mathcal{V}(\mathfrak{p}_{r+j})$ puede ser eliminado en la expresión de V. Tenemos entonces

$$V = \mathcal{V}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{V}(\mathfrak{p}_r).$$

Esta, como se puede comprobar, es la descomposición de V en componentes irreducibles dada en el Teorema (49.7.).

Subconjuntos algebraicos del plano.

El caso del plano es más sencillo y permite hacer un estudio más en profundidad. El anillo de coordenadas del plano es $K[X, Y]$. Éste es un Dominio de Factorización Única (DFU), por tanto vamos a recordar algunos de los resultados fundamentales de polinomios sobre un DFU.
Si A es un DFU, para cada polinomio $F \in A[X]$ se define el **contenido** de F como el máximo común divisor de sus coeficientes y lo representamos por $c(F)$. Un polinomio con contenido igual a 1 se llama **primitivo**.

Lema. 49.9. (Lema de Gauss.)
Sean $F, G \in A[X]$, se tiene $c(FG) = c(F)c(G)$.

DEMOSTRACIÓN. Ver la solución del Ejercicio (8.62.) □

Lema. 49.10.
Sea A un DFU con cuerpo de fracciones K. Si $F \in K[X]$ es irreducible, entonces existe $a \in A$ tal que $c(aF)^{-1}aF$ es irreducible en $A[X]$.

DEMOSTRACIÓN. Es claro que $c(aF)^{-1}aF$ tiene contenido igual a 1. Luego la única descomposición es en producto de dos polinomios no constantes: $c(aF)^{-1}aF = GH$. Entonces $F = c(aF)a^{-1}GH$ es una factorización propia, lo que es una contradicción. □

Lema. 49.11.
Sea A un DFU con cuerpo de fracciones K. Si $F \in A[X] \setminus A$ es irreducible, entonces F es irreducible en $K[X]$.

DEMOSTRACIÓN. Podemos suponer que F tiene contenido igual a 1. Supongamos que tenemos una factorización propia, $F = GH$, en $K[X]$. Para $G \in K[X]$ existe $g \in G$ tal que $gG \in A[X]$ tiene contenido igual a 1, ver Lema (49.10.), y existe $h \in A$ tal que $hH \in A[X]$ tiene también contenido igual a 1. Tenemos entonces:

$$ghF = (gG)(hH),$$

y por el Lema de Gauss, Lema (49.9.), se tiene: $gh = c(ghF) = c(gG)c(hH) = 1$, esto es, g y h son invertibles, y por tanto tenemos una factorización propia de F en $A[X]$, lo que es una contradicción.

□

Lema. 49.12.
Sea A un DFU y K su cuerpo de fracciones. Si $F \in A[X]$ se escribe en la forma $F = GH$ en $K[X]$, con $G \in A[X]$ y $c(G) \mid c(F)$, entonces $H \in A[X]$.

DEMOSTRACIÓN. Por hipótesis tenemos $F = GH$. Como $H \in K[X]$, existe $h \in A$ tal que $hH \in A[X]$ tiene contenido igual a 1. Por lo tanto $hc(F) = c(hF) = c(G(hH)) = c(G)c(hH) = c(G)$. Luego $c(F) \mid c(G)$, y como $c(G) \mid c(F)$, se tiene que h es invertible, luego $H \in A[X]$. □

Lema. 49.13.
Sea A un DFU con cuerpo de fracciones K. Si $F, G \in A[X]$ no tienen factores comunes propios en $A[X]$, entonces tampoco tienen factores comunes propios en $K[X]$.

DEMOSTRACIÓN. Suponemos que H es un factor común de F y G en $K[X]$. Sea $h \in A$ tal que $hH \in A[X]$ es primitivo. Entonces existe $F_1 \in K[X]$ tal que $(hH)F_1 = F$, y como $c(hH) = 1 \mid c(F)$, se tiene $F_1 \in A[X]$. De la misma forma existe $G_1 \in K[X]$ tal que $(hH)G_1 = G$ y se tiene $G_1 \in A[X]$. Esto es, F y G tienen un factor común en $A[X]$, lo que es una contradicción. □

Vamos a determinar todos los conjuntos algebraicos afines de $\mathbb{A}^2(K)$. Siguiendo el proceso anterior basta con determinar todos los conjuntos algebraicos irreducibles, y como consecuencia, basta determinar todos los ideales primos de $K[X]$.

Proposición. 49.14.
Sean $F, G \in K[X,Y]$ polinomios sin factores comunes, entonces $\mathcal{V}(F,G) = \mathcal{V}(F) \cap \mathcal{V}(G)$ es un conjunto finito.

Ver el Ejercicio (21.8.)

DEMOSTRACIÓN. Consideramos $F, G \in K(X)[Y]$; como no tienen factores comunes, existen $C_1, C_2 \in K(Y)[Y]$ tales que $1 = C_1F + C_2G$. Existen $D_1, D_2 \in K[X]$ tales que $D_1C_1, D_2C_2 \in K[X,Y]$, y se tiene

$$D_1D_2 = (D_1C_1)D_2F + D_1(D_2C_2)G$$

luego para cada cero común (x,y) de F y G se tiene que x es un cero de D_1D_2, y por tanto x varía en un conjunto finito. De la misma forma, usando $K(Y)[X]$, se tiene que y varía en un conjunto finito, luego el número de ceros comunes es finito. □

Corolario. 49.15.
Si $F \in K[X,Y]$ es un polinomio irreducible y $\mathcal{V}(F)$ es infinito, entonces $\mathcal{IV}(F) = (F)$ y $\mathcal{V}(F)$ es irreducible.

DEMOSTRACIÓN. Tenemos $(F) \subseteq \mathcal{IV}(F)$. Si $G \in \mathcal{IV}(F)$, entonces F y G tienen un factor común, y como F es irreducible, entonces $F \mid G$.
Si $\mathcal{V}(F) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2)$, entonces

$$(F) = \mathcal{IV}(F) = \mathcal{IV}(I_1 \cap I_2) \supseteq I_1 \cap I_2.$$

Como F es irreducible y $K[X,Y]$ es un DFU, entonces (F) es primo y existe $I_i \subseteq (F)$, luego $\mathcal{V}(F) \subseteq \mathcal{V}(I_i) \subseteq \mathcal{V}(F)$, y se tiene $\mathcal{V}(F) = \mathcal{V}(I_i)$. □

Corolario. 49.16.
Si K es un cuerpo infinito, entonces los conjuntos algebraicos irreducibles de $\mathbb{A}^2(K)$ son:

- $\mathbb{A}^2(K)$,
- $\varnothing$,
- *los conjuntos formados por un punto y*
- *las curvas planas irreducibles $\mathcal{V}(F)$, con $F \in K[X,Y]$ irreducible y $\mathcal{V}(F)$ infinito.*

DEMOSTRACIÓN. Además de $\mathbb{A}^2(K)$ y de $\varnothing$, si el conjunto algebraico irreducible es finito será un punto, y si es infinito será de la forma $V = \mathcal{V}(F_1, \ldots, F_t)$. Si $F_1, \ldots, F_t$ no tienen un factor común, entonces la misma demostración de la Proposición (49.14.) prueba que $\mathcal{V}(F_1, \ldots, F_t)$ es finito. Por tanto $F_1, \ldots, F_t$ tienen un factor común. Al considerar los polinomios $F_1, \ldots, F_t$ en $K(X)[Y]$ el factor común, F, se expresa como una combinación

$$F = C_1F_1 + \cdots + C_tF_t$$

y existe $D \in K[X]$ tal que $DC_i \in K[X, Y]$, luego tenemos la expresión

$$DF = (DC_1)F_1 + \cdots + (DC_t)F_t,$$

de donde $V = \mathcal{V}(F_1, \ldots, F_t) \subseteq \mathcal{V}(DF) = \mathcal{V}(D) \cup \mathcal{V}(F)$. Trabajando con $K(Y)[X]$ existirá un polinomio $E \in K[Y]$ tal que $V \subseteq \mathcal{V}(E) \cup \mathcal{V}(F)$. Por tanto $V \subseteq \mathcal{V}(F) \cup (\mathcal{V}(D) \cap \mathcal{V}(E))$. Como V es irreducible e infinito y $\mathcal{V}(D) \cap \mathcal{V}(E)$ es finito, se tiene $V \subseteq \mathcal{V}(F)$. Como $F \mid F_i$, se tiene $\mathcal{V}(F) \subseteq \mathcal{V}(F_i)$, luego $\mathcal{V}(F) \subseteq \cap_i \mathcal{V}(F_i) = \mathcal{V}(F_1, \ldots, F_t) = V$, y tenemos la igualdad $V = \mathcal{V}(F)$. Una factorización $F = F_1^{e_1} \cdots F_t^{e_t}$ produce una descomposición $\mathcal{V}(F) = \mathcal{V}(F_1) \cup \ldots \cup \mathcal{V}(F_t)$, luego $t = 1$ y $\mathcal{V}(F) = \mathcal{V}(F_1)$ es irreducible e infinito. El Corolario anterior nos dice que entonces $\mathcal{V}(F)$ es irreducible. □

Corolario. 49.17.
Si K es un cuerpo algebraicamente cerrado y $F \in K[X, Y]$ con $F = F_1^{e_1} \cdots F_r^{e_r}$ es una descomposición en irreducibles, entonces $\mathcal{V}(F) = \mathcal{V}(F_1) \cup \cdots \cup \mathcal{V}(F_r)$ es la descomposición de $\mathcal{V}(F)$ en componentes irreducibles y además $\mathcal{IV}(F) = (F_1, \ldots, F_r)$.

DEMOSTRACIÓN. Ya que la descomposición se deduce de la definición, basta ver que en este caso un conjunto algebraico V es irreducible si y solo si existe un polinomio irreducible F tal que $V = \mathcal{V}$ o $V = \mathcal{V}(X - a, Y - b)$ para $a, b \in K$.

Si V es irreducible y finito, entonces se reduce a un punto, y por tanto es de la forma $\mathcal{V}(X - a, Y - b)$. El recíproco es cierto.

Si V es infinito podemos usar la demostración del Corolario anterior y obtenemos que $V = \mathcal{V}(F)$ para algún F irreducible.

Si F es irreducible, y $V = \mathcal{V}(F) = \mathcal{V}(I_1) \cup \mathcal{V}(I_2) = \mathcal{V}(I_1 \cap I_2)$, entonces $(F) = \mathcal{IV}(F) = \mathcal{IV}(I_1 \cap I_2) = I_1 \cap I_2$ y se tiene $(F) = I_1$ ó $(F) = I_2$. Luego $V = \mathcal{V}(I_1)$ o $V = \mathcal{V}(I_2)$. □

50. Teorema de Lasker–Noether para anillos de polinomios

En las secciones anteriores hemos supuesto que los ideales con los que trabajábamos tenían una descomposición primaria; se trata ahora de probar que en el caso de anillos noetherianos todo ideal propio tiene una descomposición primaria.
Un ideal propio $\mathfrak{a}$ de un anillo A es **irreducible** si para cada descomposición $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$ se tiene $\mathfrak{a} = \mathfrak{a}_1$ o $\mathfrak{a} = \mathfrak{a}_2$.

Lema. 50.1.
Cada ideal irreducible de un anillo noetheriano es primario.

DEMOSTRACIÓN. Si $\mathfrak{a}$ es un ideal irreducible y $ab \in \mathfrak{a}$ con $a \notin \mathfrak{a}$, consideramos $(\mathfrak{a} : b^n)$ y la cadena

$$\mathfrak{a} \subseteq (\mathfrak{a} : b) \subseteq (\mathfrak{a} : b^2) \subseteq (\mathfrak{a} : b^3) \subseteq \cdots$$

Por ser A noetheriano, existe n tal que $(\mathfrak{a} : b^n) = (\mathfrak{a} : b^{n+1})$. Consideramos la intersección $(\mathfrak{a} + (b^n)) \cap (\mathfrak{a} + (a))$. Vamos a ver que es igual a $\mathfrak{a}$. Si $x \in (\mathfrak{a} + (b^n)) \cap (\mathfrak{a} + (a))$, entonces

$$x = a_1 + c_1 b^n = a_2 + c_2 a, \quad a_1, a_2 \in \mathfrak{a}, \quad c_1, c_2 \in A.$$

Multiplicando por b se tiene:

$$xb = a_1 b + c_1 b^{n+1} = a_2 b + c_2 ab \in \mathfrak{a}$$

Entonces $c_1 \in (\mathfrak{a} : b^{n+1}) = (\mathfrak{a} : b^n)$, y $x = a_1 + c_1 b^n \in \mathfrak{a}$.
Ahora como $\mathfrak{a}$ es irreducible, resulta $\mathfrak{a} = \mathfrak{a} + (b^n)$, y por tanto $b^n \in \mathfrak{a}$. □

Teorema. 50.2. (Teorema de Lasker–Noether)
Sea K un cuerpo. Cada ideal de $A = K[X_1, \ldots, X_n]$ tiene una descomposición primaria.

DEMOSTRACIÓN. [1] Veamos que cada ideal propio, $\mathfrak{a}$, es una intersección finita de ideales irreducibles. Llamamos $\Gamma = \{\mathfrak{b} \subseteq A/\mathfrak{a} \mid \ \mathfrak{b}$ no es intersección fin. de id. irred.$\}$. Como $A/\mathfrak{a}$ es noetheriano, existe elementos maximales en Γ. Sea $\mathfrak{b} \in \Gamma$ maximal. Como $\mathfrak{b}$ no es irreducible, existen ideales $\mathfrak{b}_1$ y $\mathfrak{b}_2$ tales que $\mathfrak{b} = \mathfrak{b}_1 \cap \mathfrak{b}_2$, con $\mathfrak{b} \subsetneqq \mathfrak{b}_1$ y $\mathfrak{b} \subsetneqq \mathfrak{b}_2$. Entonces $\mathfrak{b}_i$ no pertenece a Γ y es una intersección finita de ideales irreducibles, luego $\mathfrak{b}$ también lo es, lo que es una contradicción. Por tanto $\Gamma = \varnothing$. En particular 0 es una intersección finita de ideales irreducibles de $A/\mathfrak{a}$, y tenemos que $\mathfrak{a}$ es una intersección finita de ideales irreducibles de A.
Por el Lema (50.1.) tenemos que $\mathfrak{a}$ es una intersección finita de ideales primarios. □

[1] Fue Lasker quien en 1905 prueba este resultado para el anillo $\mathbb{Z}[X]$; fue Noether quien en 1920 introduce la condición de anillo con condición de cadena ascendente y prueba su utilidad en la demostración de este teorema.

51. Ejercicios

Descomposición primaria de ideales

Ejercicio. 51.1.
Sea $f : A \to B$ un homomorfismo de anillos, $\mathfrak{q}$ un ideal $\mathfrak{p}$–primario de B. Prueba:

(1) $f^{-1}(\mathfrak{p})$ es un ideal primo de A.
(2) $f^{-1}(\mathfrak{q})$ es un ideal $f^{-1}(\mathfrak{p})$–primario de A.

SOLUCIÓN

Ejercicio. 51.2.
Sea $f : A \longrightarrow B$ un homomorfismo sobreyectivo de anillos conmutativos y $\mathfrak{a}$ un ideal de A que contiene a $\operatorname{Ker}(f)$. Prueba que son equivalentes:

(a) $\mathfrak{a}$ es primario.
(b) $f(\mathfrak{a})$ es primario.

Y que en este caso si el primo asociado a $\mathfrak{a}$ es $\mathfrak{p}$, el primo asociado a $f(\mathfrak{a})$ es $f(\mathfrak{p})$.

SOLUCIÓN

Ejercicio. 51.3. (AM, Cap 4, Ej 2)
Si $\mathfrak{a} = \operatorname{rad}(\mathfrak{a})$, entonces $\mathfrak{a}$ no tiene ideales primos inmersos (embebidos).

SOLUCIÓN

Ejercicio. 51.4. (AM, Cap 4, Ej 4)
En el anillo de polinomios $\mathbb{Z}[T]$, el ideal $\mathfrak{m} = (2, T)$ es maximal y el ideal $\mathfrak{q} = (4, T)$ es $\mathfrak{m}$–primario, pero no es una potencia de $\mathfrak{m}$.

SOLUCIÓN

Ejercicio. 51.5. (AM, Cap 4, Ej 5)
En el anillo de polinomios $K[X, Y, Z]$, donde K es un cuerpo y X, Y y Z son indeterminadas independientes, sea $\mathfrak{p}_1 = (X, Y)$, $\mathfrak{p}_2 = (X, Z)$, $\mathfrak{m} = (X, Y, Z)$; $\mathfrak{p}_1$ y $\mathfrak{p}_2$ son primos y $\mathfrak{m}$ es maximal. Sea $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$.

Probar que $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ *es una descomposición primaria reducida de* $\mathfrak{a}$*. ¿Cuáles son las componentes aisladas y cuáles las inmersas (embebidas)?*

SOLUCIÓN

Ejercicio. 51.6. (AM, Cap 4, Ej 7)
Sea A *un anillo y sea* $A[X]$ *el anillo de polinomios en una indeterminada sobre* A*. Para cada ideal* $\mathfrak{a}$ *de* A*, sea* $\mathfrak{a}[X]$ *el conjunto de todos lospolinomios en* $A[X]$ *con coeficientes en* $\mathfrak{a}$*.*

(1) $\mathfrak{a}[X]$ *es la extensión de* $\mathfrak{a}$ *a* $A[X]$*.*
(2) Si $\mathfrak{p}$ *es un ideal primo en* A*, entonces* $\mathfrak{p}[X]$ *es un ideal primo en*$A[X]$*.*
(3) Si $\mathfrak{q}$ *es un ideal* $\mathfrak{p}$*–primario en* A*, entonces* $\mathfrak{q}[X]$ *es un ideal* $\mathfrak{p}[X]$*–primario en* $A[X]$*.*
Pista: utilizar Capítulo I, Ejercicio 2.
(4) Si $\mathfrak{a} = \cap_{i=1}^{n} \mathfrak{q}_i$ *es una descomposición minimal primaria en* A*, entonces* $\mathfrak{a}[X] = \cap_{i=1}^{n} \mathfrak{q}_i[X]$ *es una descomposición minimalprimaria en* $A[X]$*.*
(5) Si $\mathfrak{p}$ *es un ideal primo minimal de* $\mathfrak{a}$*, entonces* $\mathfrak{p}[X]$ *es un ideal primo minimal de* $\mathfrak{a}[X]$*.*

SOLUCIÓN

Ejercicio. 51.7. (AM, Cap 4, Ej 8)
Sea k *un cuerpo. Probar que en el anillo de polinomios* $k[X_1, \ldots, X_n]$ *los ideales* $\mathfrak{p}_i = (X_1, \ldots, X_i)$ *(*$1 \leq i \leq n$*) son primos y todas sus potencias son primarias.*

Pista: utilizar el Ejercicio (51.6.).

SOLUCIÓN

Ejercicio. 51.8. (AM, Cap 4, Ej 9)
En un anillo A*, sea* $\mathcal{D}(A)$ *el conjunto de ideales primos* $\mathfrak{p}$ *que satisfacen la siguiente condición: existe* $a \in A$ *tal que* $\mathfrak{p}$ *es minimal en el conjunto de los ideales primos que contienen* $(0 : a)$*.*

(1) Probar que $x \in A$ *es un divisor de cero si y sólo si* $x \in \mathfrak{p}$ *para algún* $\mathfrak{p} \in \mathcal{D}(A)$*.*
(2) Sea S *un subconjunto multiplicativamente cerrado de* A*, y se identifica* $\operatorname{Spec}(S^{-1}A)$ *con su imagen en* $\operatorname{Spec}(A)$ *(Capítulo 3, Ejercicio 21). Probar que* $\mathcal{D}(S^{-1}A) = \mathcal{D}(A) \cap \operatorname{Spec}(S^{-1}A)$*.*
(3) Si el ideal cero tiene una descomposición primaria, probar que $\mathcal{D}(A)$ *es el conjunto de los ideales primos asociados de 0.*

SOLUCIÓN

Ejercicio. 51.9. (AM, Cap 4, Ej 10)
Para cada ideal primo $\mathfrak{p}$ en un anillo A, sea $S_{\mathfrak{p}}(0)$ el núcleo del homomorfismo $A \longrightarrow A_{\mathfrak{p}}$. Probar que:

(1) $S_{\mathfrak{p}}(0) \subseteq \mathfrak{p}$.
(2) $\operatorname{rad}(S_{\mathfrak{p}}(0)) = \mathfrak{p}$ *si, y sólo si,* $\mathfrak{p}$ *es un ideal minimal primo de* A.
(3) Si $\mathfrak{p} \supseteq \mathfrak{p}'$, *entonces* $S_{\mathfrak{p}}(0) \subseteq S_{\mathfrak{p}'}(0)$.
(4) En el caso en que el ideal 0 tiene una descomposición primaria se tiene: $\cap_{\mathfrak{p}\in\mathcal{D}(A)} S_{\mathfrak{p}}(0) = 0$, *donde* $\mathcal{D}(A) = \{\mathfrak{p} \mid \exists a \in A$ *tal que* $\mathfrak{p}$ *es minimal en el conjunto de los ideales primos que contienen a* $(0 : a)\}$.

Tenemos que $S_{\mathfrak{p}}(0)$ *es la saturación de 0 con respecto a* $\mathfrak{p}$ *ó, equivalentemente, con respecto a* $A \setminus \mathfrak{p}$. *Ver ejercicio* (51.13.).

SOLUCIÓN

Ejercicio. 51.10.
Se considera el ideal $\mathfrak{a} = (2X, X^2) \subseteq \mathbb{Z}[X]$.

(1) Prueba que $\mathfrak{a}$ *no es un ideal primario.*
(2) Como $(X)^2 \subseteq \mathfrak{a}$, *este ejemplo también prueba que si un ideal contiene una potencia de un ideal primo no necesariamente es primario.*
(3) Prueba que $(2X, X^2) = (X) \cap (X^2, 2) = (X) \cap (X^2, 2+X) = (X) \cap (X^2, 2X, 4)$ *son descomposiciones primarias de* $\mathfrak{a}$.
(4) ¿Cuáles son los ideales primos asociados?

SOLUCIÓN

Ejercicio. 51.11.
Determina los ideales primos minimales sobre $\mathfrak{a} = (XY, YZ + XZ) \subseteq K[X, Y, Z]$, *y prueba que* $\operatorname{rad}(XY, YZ + XZ) = (XY, XZ, YZ)$.

SOLUCIÓN

Ejercicio. 51.12.
Sea A *un DFU y* $\mathfrak{a} = (a) \subseteq A$ *un ideal principal, son equivalentes:*

(a) $\mathfrak{a}$ *es primario,*
(b) Existen $p \in A$ *primo,* $u \in A$ *invertible, y* $e \in \mathbb{N}$ *tales que* $a = up^e$.

Por tanto se tiene $\mathfrak{a} = (p)^e$.

SOLUCIÓN

Ejercicio. 51.13.
*Sea A un anillo conmutativo y sea Σ un subconjunto multiplicativo. Para cada ideal $\mathfrak{a}$ representamos por $\mathrm{Sat}_\Sigma(\mathfrak{a})$ a la contracción del ideal $\Sigma^{-1}\mathfrak{a}$. El ideal $\mathrm{Sat}_\Sigma(\mathfrak{a})$ se llama **saturación** de $\mathfrak{a}$ respecto a Σ.*

(1) Demuestra que $\mathrm{Sat}_\Sigma(\mathfrak{a}) \cap \mathrm{Sat}_\Sigma(\mathfrak{b}) = \mathrm{Sat}_\Sigma(\mathfrak{a} \cap \mathfrak{b})$.
(2) Demuestra que $\mathrm{Sat}_\Sigma(\mathrm{rad}(\mathfrak{a})) = \mathrm{rad}(\mathrm{Sat}_\Sigma(\mathfrak{a}))$.
(3) Demuestra que $\mathrm{Sat}_\Sigma(\mathfrak{a}) = A$ si, y sólo si, $\mathfrak{a} \cap \Sigma \neq \varnothing$.
(4) Demuestra que $\mathrm{Sat}_{\Sigma_1}(\mathrm{Sat}_{\Sigma_2}(\mathfrak{a})) = \mathrm{Sat}_{\Sigma_1\Sigma_2}(\mathfrak{a})$.
(5) Supongamos que $\mathfrak{a}$ admite una descomposición primaria. Demuestra que el conjunto de los ideales $\mathrm{Sat}_\Sigma(\mathfrak{a})$, donde Σ recorre todos los subconjuntos multiplicativos de A, es finito.

SOLUCIÓN

Ejercicio. 51.14.
Se considera la aplicación $f : \mathbb{Q}[X,Y,Z] \to \mathbb{Q}[T]$, definida por

$$f(X) = T^3, \qquad f(Y) = T^4, \qquad f(Z) = T^5.$$

(1) Prueba que el núcleo de f es $\mathfrak{p} = (Y^2 - XZ, YZ - X^3, Z^2 - X^2Y)$.
(2) Prueba que $\mathfrak{p}$ es un ideal primo.
(3) Razona que el radical de $\mathfrak{p}^2$ es igual a $\mathfrak{p}$.
(4) ¿Cuántos elementos tiene una base de Groebner reducida de $\mathfrak{p}^2$?
(5) Estudia el elemento $Y(X^5 + XY^3 - 3X^2YZ + Z^3)$, y razona que $\mathfrak{p}^2$ no es un ideal primario.

SOLUCIÓN

Ejercicio. 51.15.
Sea A un anillo conmutativo noetheriano y $\mathfrak{a}$ un ideal. Demuestra que $\mathfrak{a}$ es radical si y sólo si todas sus componentes primarias en una descomposición primaria minimal son ideales primos. Deduce que la descomposición primaria minimal de un ideal radical es única.

SOLUCIÓN

Ejercicio. 51.16.
Sea A un anillo conmutativo noetheriano y sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ los primos asociados del ideal 0.

(1) Demuestra que $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_m$ es el conjunto de elemento nilpotentes de A.
(2) Demuestra que $\mathfrak{p}_1 \cup \ldots \cup \mathfrak{p}_m$ es el conjunto de divisores de cero de A.

SOLUCIÓN

Ejercicio. 51.17.
Si $\mathfrak{q}_1, \mathfrak{q}_2$ son ideales $\mathfrak{m}$–primarios ($\mathfrak{m}$ es un ideal maximal), prueba que los ideales $\mathfrak{q}_1 + \mathfrak{q}_2$ y $\mathfrak{q}_1\mathfrak{q}_2$ son también $\mathfrak{m}$–primarios.

SOLUCIÓN

Ejercicio. 51.18.
Sea A el conjunto de todas las sucesiones de elementos de $\mathbb{Z}_2$ eventualmente constantes; A es un anillo con las operaciones definidas componente a componente.

Sea $\mathfrak{p}_n$ el conjunto de los elementos de A con término n igual a cero, y sea $\mathfrak{p}_0$ el conjunto de las sucesiones con un número finito de elementos no nulos.

(1) $\mathfrak{p}_n$ es un ideal primo para $n \geq 0$.
(2) Todo ideal primo de A es de la forma $\mathfrak{p}_n$ para $n \in \mathbb{N}$.
(3) Todo ideal primario de A es un ideal primo.
(4) $\cap\{\mathfrak{p}_n \mid n \geq 1\} = 0$ y $\mathfrak{p}_0 \cap (\cap\{\mathfrak{p}_i \mid n \geq 1, n \neq i\}) \neq 0$. Como consecuencia 0 no es una intersección finita de ideales primarios.
(5) Ya que A no es un anillo noetheriano, construye un ideal que no es finitamente generado, y construye una cadena estrictamente ascendente de ideales de A.

SOLUCIÓN

Ejercicio. 51.19.
Sea A un anillo, $\mathfrak{a} \subseteq A$ un ideal de A tal que existe una descomposición en irreducibles $\mathfrak{a} = \mathfrak{b}_1 \cap \ldots, \cap \mathfrak{b}_t$, con $b_j \nsubseteq \cap_{i \neq j} \mathfrak{b}_i$, para cada índice j.

(1) Sea $\mathfrak{a} = \mathfrak{c}_1 \cap \ldots \cap \mathfrak{c}_t$ una descomposición en irreducibles con $\mathfrak{c}_i \subseteq \mathfrak{b}_i$. Prueba que $\mathfrak{c}_i = \mathfrak{b}_i$ para cada índice i.
(2) Sea $\mathfrak{a} = \mathfrak{c}_1 \cap \ldots \cap \mathfrak{c}_s$ una descomposición en irreducibles con $\mathfrak{c}_j \nsubseteq \cap_{i \neq j} \mathfrak{c}_i$, para cad índice j. Para cada índice $i = 1, \ldots, t$ definimos $\mathfrak{d}_i = \mathfrak{b}_1 \cap \ldots \cap \widehat{\mathfrak{b}_i} \cap \ldots \cap \mathfrak{b}_t$. Prueba que para cada índice i existe un índice j tal que $\mathfrak{a} = \mathfrak{b}_i \cap \mathfrak{c}_j$.
(3) Prueba que $t = s$.

SOLUCIÓN

Ejercicio. 51.20. (Patologías de la descomposición primaria)
Sea K un cuerpo y $\mathbb{Z}$ el anillo de los enteros.

(1) *Un ideal primario no es necesariamente una potencia de un ideal primo. El ideal $(X, Y^2) \subseteq K[X,Y]$ es un ideal primario con radical (X,Y).*
(2) *Un ideal primario no es necesariamente una potencia de un ideal primo. El ideal $(4, X) \subseteq \mathbb{Z}[X]$ es primario con radical $(2, X)$.*
(3) *Un ideal con radical primo no es necesariamente primario. El ideal $(X^2, XY) \subseteq K[X,Y]$ no es primario y su radical es (X).*
(4) *Un ideal con radical primo no es necesariamente primario. El ideal $(X^2, 2X) \subseteq \mathbb{Z}[X]$ no es primario, y su radical es (X).*
(5) *Un ideal en un anillo noetheriano puede tener infinitas descomposiciones primarias. Para cada $k \in K$ el ideal $(Y - kX, X^2)$ es un ideal primario con radical (X,Y). Si $k \neq k'$, entonces $(Y - kX, X^2) \neq (Y - k'X, X^2)$, y se tiene que $(X^2, XY) = (X) \cap (Y - kX, X^2)$ es una descomposición primaria reducida.*
(6) *Un ideal primario no necesariamente irreducible. El ideal $(4, 2X, X^2) \subseteq \mathbb{Z}[X]$ es primario, y se tiene $(4, 2X, X^2) = (4, X) \cap (2, X^2)$.*
(7) *Una potencia de un ideal primo no es necesariamente primario. Se considera el subanillo A de $\mathbb{Z}[X]$ formado por todos los polinomios con término lineal, el coeficiente de X, divisible por 3. En A el ideal $\mathfrak{p} = (3X, X^2, X^3)$ es un ideal primo, pero $\mathfrak{p}^2$ no es primario.*

SOLUCIÓN

Ejercicio. 51.21.
Razona que un ideal primo $\mathfrak{p}$ contiene a un ideal $\mathfrak{a}$ (que tiene una descomposición primaria) si, y sólo si, $\mathfrak{p}$ contiene a uno de los primos asociados de una descomposición primaria minimal de $\mathfrak{a}$.

SOLUCIÓN

Ejercicio. 51.22.
Sean $\mathfrak{a}, \mathfrak{b}$ ideales de un anillo conmutativo A, $\mathfrak{a}$ propio, y sea $(\mathfrak{a} : \mathfrak{b}) = \{x \in A \mid x\mathfrak{b} \subseteq \mathfrak{a}\}$. Se tiene $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$. Demuestra que si A es noetheriano, son equivalentes:

(a) $\mathfrak{a} = (\mathfrak{a} : \mathfrak{b})$.
(b) *$\mathfrak{b}$ no está contenido en ninguno de los ideales primos asociados de $\mathfrak{a}$.*

SOLUCIÓN

Ejercicio. 51.23.
Sea A un anillo conmutativo y $\mathfrak{q}$ un ideal $\mathfrak{p}$–primario. Sea $\mathfrak{a}$ un ideal cualquiera de A. Prueba:

(1) Si $\mathfrak{a} \subseteq \mathfrak{q}$, entonces $(\mathfrak{q} : \mathfrak{a}) = A$.
(2) Si $\mathfrak{a} \nsubseteq \mathfrak{p}$, entonces $(\mathfrak{q} : \mathfrak{a}) = \mathfrak{q}$.
(3) Si $\mathfrak{a} \subseteq \mathfrak{p}$ y $\mathfrak{a} \nsubseteq \mathfrak{q}$, entonces $\mathfrak{q} \subsetneq (\mathfrak{q}; \mathfrak{a}) \subsetneq A$.
(4) Sea $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t$ una descomposición primaria minimal donde cada $\mathfrak{q}_i$ es $\mathfrak{p}_i$–primario.
(5) Para cualquier ideal $\mathfrak{b}$ de A se tiene $(\mathfrak{a} : \mathfrak{b}) = \mathfrak{a}$ si y sólo si $\mathfrak{b} \nsubseteq \mathfrak{p}_i$ para todo índice i.

SOLUCIÓN

Ejercicio. 51.24.
Sean $\mathfrak{q}_i$, $i = 1, 2$, dos ideales $\mathfrak{p}_i$–primarios de un anillo conmutativo A tales que $\mathfrak{p}_1 \nsubseteq \mathfrak{p}_2 \nsubseteq \mathfrak{p}_1$.

(1) Demuestra que $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ no es primario.
(2) Sean $a, b \in A$ tales que $ab \in \mathfrak{a}$. Demuestra que existen $r, s \in \mathbb{N}$ tales que $a^r, b^s \in \mathfrak{a}$.

SOLUCIÓN

Ejercicio. 51.25.
Sean $\mathfrak{a}, \mathfrak{b}, \mathfrak{q}$ ideales de un anillo conmutativo A tales que $\mathfrak{q}$ es primario, $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}$ y $\mathfrak{a} \nsubseteq \mathfrak{q}$. Demuestra que $\mathfrak{b} \subseteq \operatorname{rad}(\mathfrak{q})$.

SOLUCIÓN

Conjuntos algebraicos irreducibles

Teorema de Lasker–Noether para anillos de polinomios

Ejercicio. 51.26.
Sobre cálculo de descomposiciones primarias.

(1) Halla todas las descomposiciones primarias de (X^2, XY) en $K[X, Y]$ siendo K un cuerpo.
(2) Halla todas las descomposiciones primarias de (X^2, XY) en $\mathbb{Z}[X, Y]$.

SOLUCIÓN

Ejercicio. 51.27.
Sea $\mathfrak{a} = (XY, X - YZ) \subseteq K[X,Y,Z]$. *Demuestra que* $\mathfrak{a} = (X,Z) \cap (Y^2, X - YZ)$ *es una descomposición primaria reducida de* $\mathfrak{a}$.

SOLUCIÓN

Capítulo X

Dominios de Dedekind

Introducción

El tema central de este capítulo lo constituyen los Dominios de Dedekind, que son los dominios noetherianos de dimensión uno íntegramente cerrados; aquí vamos a hacer un tratamiento algebraico de los mismos a partir de los Dominios de Valoración Discreta. El objetivo del capítulo es caracterizar los dominios en estas dos clases y observar que los Dominios de Dedekind aparecen de forma natural al considerar los anillos de enteros algebraicos.

52. Dominios de valoración discreta

Dado un cuerpo K una **valoración discreta** v sobre K es una aplicación sobreyectiva[1] $v\colon K^* \to \mathbb{Z}$, $K^* = K \setminus \{0\}$, verificando:
(I) $v(xy) = v(x) + v(y)$.
(II) $v(x+y) \geq \min\{v(x), v(y)\}$.

También se puede considerar la aplicación v definida sobre todo K agregando a $\mathbb{Z}$ un elemento $\{+\infty\}$, verificando $n < +\infty$ para cada $n \in \mathbb{Z}$, y definiendo $v(0) = +\infty$.
Si v es una valoración discreta sobre K, llamamos **dominio de valoración discreta** de v al conjunto

$$D = \{r \in K \mid \ v(r) \geq 0\} \cup \{0\}.$$

Lema. 52.1.
Se verifican las siguientes propiedades:
(1) D es un subanillo de K.
(2) Las unidades de D son los elementos x que verifican $v(x) = 0$.
(3) D es un anillo local con ideal maximal $\mathfrak{m} = \{x \in D \mid \ v(x) > 0\} \cup \{0\}$.

DEMOSTRACIÓN. (1). Si $x, y \in D \setminus \{0\}$, entonces $v(x)$, $v(y) \geq 0$, y se verifica:

$$v(x+y) \geq \min\{v(x), v(y)\} \geq 0.$$

$$v(xy) = v(x) + v(y) \geq 0.$$

Por otro lado se verifica:

$$v(1) = v(1 \cdot 1) = v(1) + v(1), \text{ luego } v(1) = 0.$$

(2). Si $x \in D$ es una unidad, entonces existe $y \in D$ tal que $xy = 1$, luego $0 = v(1) = v(xy) = v(x) + v(y)$, y por tanto $v(x) = 0 = v(y)$. Recíprocamente, si $x \in D$ y $v(x) = 0$, entonces tomamos $x^{-1} \in K$, se verifica $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1}) = v(x^{-1})$, luego $x^{-1} \in D$ y x es una unidad en D.
(3). Si $0 \neq a \in D$ no es invertible, entonces $v(a) > 0$. Luego solo falta probar que $\mathfrak{m}$ es un ideal. Dados $a, b \in \mathfrak{m}$, se tiene $v(a+b) \geq \min\{v(a), v(b)\} > 0$, luego $a + b \in \mathfrak{m}$. □

Ejercicio. 52.2.
Dos elementos $a, b \in D$ verifican $v(a) = v(b)$ si, y solo si, existe un elemento invertible $u \in D$ tal que $a = bu$.

[1] Podríamos definir valoraciones discretas sin necesidad de imponer la condición de sobreyectiva para después hacer un proceso de normalización por el que pasaríamos a considerar finalmente aplicaciones sobreyectivas.

En general un **dominio de valoración discreta** es un dominio D que es el dominio de valoración discreta de alguna valoración v sobre su cuerpo de fracciones K.

Ejemplo. 52.3.
El ejemplo más conocido de valoración discreta es la **valoración** p**–ádica** en $\mathbb{Q}$, siendo p un número entero primo. Esta valoración se representa por v_p, y está definida para cada número racional no nulo r por $v_p(r) = e \in \mathbb{Z}$, donde e es el exponente de p en la expresión de r como producto de factores primos. El anillo de valoración discreta es: $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid p \nmid b\}$, esto es, el localizado de $\mathbb{Z}$ en el ideal primo (p).

Este ejemplo se puede extender a considerar un anillo de polinomios sobre una indeterminada con coeficientes en un cuerpo.

Ejemplo. 52.4.
Dado un cuerpo L y un polinomio irreducible $F \in L[X]$ se considera la aplicación $v_F : L(X)^* \to \mathbb{Z}$ definida $v_F(G/H) = e$, siendo G/H irreducible, y e la mayor potencia de F que divide a G o $-e$ la mayor potencia de F que divide a H.

Se tiene que v_F es una valoración discreta y el anillo de valoración asociado, al igual que en el caso p–ádico, está formado por las fracciones irreducibles en $L(X)$ cuyo denominador no es múltiplo de F.

Ejemplo. 52.5.
Consideramos $\mathbb{R}[X]$, y la valoración v_X sobre $\mathbb{R}(X)$. El anillo de valoración discreta es: $D = \{F/G \mid G(0) \neq 0\}$. Sabemos que D se puede identificar con el anillo de funciones racionales valoradas en $\mathbb{R}$ en un entorno de cero de la recta real. El ideal maximal es el generado por (X), y X es el único elemento irreducible. Observa que para cada $f \in D$ se tiene que $v_X(f)$ indica el orden de la función f en el punto 0.

Ejemplo. 52.6.
Dado un cuerpo K, se considera $K[[X]]$, el anillo de las series formales de potencias, y $K((X))$, su cuerpo de fracciones. Se tiene una valoración v en $K((X))$, definida $v(F/G) = e$, siendo X^e la mayor potencia de X que divide a F/G. El anillo de valoración es $K[[X]]$.

Aún otro ejemplo.

Ejemplo. 52.7.
El conjunto $L((X))$ de las series de Laurent tiene como elementos a las series formales $\sum_{i=t}^{\infty} a_i X^i$, con $a_t \neq 0$, con $t \in \mathbb{N}$. Si llamamos K al cuerpo de fracciones, existe una valoración discreta $v : K \to \mathbb{Z}$ definida:

$$v(\sum_{i=t}^{\infty} a_i X^i) = t.$$

El anillo de valoración para esta valoración es el anillo de las series formales: $\sum_{i=0}^{\infty} a_i X^i$.

Observación. 52.8.
Observa que si D es un dominio de valoración discreta, entonces se verifica:

(1) Para cada $0 \neq a \in D$ se tiene $v(a) = 0$ si, y solo si, a es invertible en D.
(2) Para cada $0 \neq a \in K$ se tiene $a \in D$, o $a^{-1} \in D$.
(3) Si $a, b \in D$ verifican $v(a) = v(b)$, entonces $aD = bD$.

DEMOSTRACIÓN. (1). Observa que $v(1) = v(1) + v(1)$, luego $v(1) = 0$. Si a es invertible en D, se tiene $0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1})$ y por tanto $v(a^{-1}) = -v(a)$. Como ambos son no negativos, se tiene $v(a) = 0 = v(a^{-1})$. Recíprocamente, si $v(a) = 0$, como $a^{-1} \in K$, y se tiene $0 = v(1) = v(aa^{-1}) = v(a) + v(a^{-1})$, se tiene $v(a^{-1}) = 0$ y por tanto $a^{-1} \in D$.

(2). Si $a \notin D$, entonces $v(a) < 0$, luego $v(a^{-1} = -v(a) > 0$ y por tanto $a^{-1} \in D$.

(3). Si $v(a) = v(b)$, entonces $v(ab^{-1}) = 0$, luego $ab^{-1} \in D$ y es invertible. Entonces $aD = bD$. □

Lema. 52.9.
Todo dominio de valoración discreta es un DE (dominio euclídeo).
Como consecuencia, todo dominio de valoración discreta es un DIP, un DFU, y es íntegramente cerrado.

DEMOSTRACIÓN. Basta ver que la aplicación v restringida a D define una función euclídea. Dados $a, b \in D$, si $v(a) < v(b)$, entonces la división es: $a = 0b + a$. Si $v(a) \geq v(b)$, existe $c \in D$ tal que $v(a) = v(b) + v(c)$, por ser v sobreyectiva. Entonces $v(a) = v(bc)$ y se tiene $aD = bcD$, luego existe un elemento invertible $u \in D$ tal que $a = bcu$, y la división es: $a = b(cu) + 0$. □

Observa que esta demostración en realidad prueba que si $a, b \in D$ son elementos no nulos, entonces $a|b$ ó $b|a$.

Si D es un dominio de valoración discreta, entonces es un anillo local con ideal maximal $\mathfrak{m} = \{a \in D \mid v(a) > 0\}$. Como todo dominio de valoración discreta es un DIP, sea $\mathfrak{m} = tD$. Cada elemento $0 \neq a \in D$ verifica $v(a) \geq 0$, sea $v(a) = r$. Si $r = 0$, entonces a es invertible. Si $r > 0$, entonces $a \in \mathfrak{m} = tD$, y existe $d \in D$ tal que $a = td$. Se verifica $v(a) = v(t) + v(d)$, y por tanto $v(a) \geq v(t)$. Por ser v sobreyectiva existe $b \in D$ tal que $v(b) = 1$, lo que implica que $v(t) = 1$. Todo elemento $a \in D$ tal que $v(a) = 0$ es invertible, y si $v(a) = 1$, entonces $a = tu$, siendo $u \in D$ invertible. Por inducción se tiene que para cada $o \neq a \in D$ se tiene $a = t^{v(a)}u$, siendo $u \in D$ invertible. El elemento t se llama un **parámetro de uniformización** o **parámetro local** de D.

En lo que sigue, para un dominio local D con ideal maximal $\mathfrak{m}$, llamamos K al cuerpo de fracciones de D, y F al cuerpo residual $D/\mathfrak{m}$.

Proposición. 52.10.
Si D es un dominio de valoración discreta con ideal maximal $\mathfrak{m} = tD$, entonces cada elemento $0 \neq a \in D$ se escribe, de forma única, como $a = t^r u$, siendo $r \in \mathbb{N}$ y $u \in D$ invertible.
En particular

(1) todo elemento no nulo de K se escribe de forma única como $t^s u$, siendo $s \in \mathbb{Z}$ y $u \in D$ invertible;
(2) todo ideal no nulo de D es el ideal principal generado por t^r para algún $r \in \mathbb{N} \setminus \{0\}$, por lo tanto los ideales de D forman una cadena descendente y D es un anillo noetheriano;
(3) los únicos ideales primos de D son 0 y $\mathfrak{m}$.

Teorema. 52.11.
Sea D un dominio. Las siguientes propiedades son equivalentes:

(a) D es un dominio de valoración discreta que no es un cuerpo.
(b) D es un dominio local noetheriano de dimensión uno íntegramente cerrado.
(c) D es un dominio local noetheriano de dimensión uno y el ideal maximal es principal.
(d) D es un dominio local noetheriano de dimensión uno verificando

$$\dim_F(\mathfrak{m}/\mathfrak{m}^2) = 1.$$

(Donde $F = R/\mathfrak{m}$ y $\mathfrak{m}$ es el ideal maximal.)
(e) D es un dominio local que no es un cuerpo y cada ideal no nulo es una potencia del ideal maximal.
(f) D es un dominio que no es un cuerpo y cada ideal no nulo es de la forma (x^α) para algún $x \in D$.
(g) D es un dominio de ideales principales local que no es un cuerpo.
(h) D es un dominio de valoración noetheriano que no es un cuerpo.

DEMOSTRACIÓN. (c) $\Rightarrow$ (d). Supongamos que $\mathfrak{m} = (x)$, entonces $\{x+\mathfrak{m}\}$ es un sistema de generadores de $\mathfrak{m}/\mathfrak{m}^2$ y por tanto $\dim_F(\mathfrak{m}/\mathfrak{m}^2) \leq 1$. Si $\mathfrak{m} = \mathfrak{m}^2$, entonces $x = dx^2$ para algún $d \in D$, esto es $1 = dx$, luego x es una unidad si es no nulo ó bien $x = 0$. En cualquier caso llegamos a una contradicción ya que la dimensión de D es positiva. En consecuencia $\dim_F(\mathfrak{m}/\mathfrak{m}^2) = 1$.

(d) $\Rightarrow$ (e). Sea $0 \neq \mathfrak{a} \leq D$ un ideal no nulo, entonces $\operatorname{rad}(\mathfrak{a}) = \mathfrak{m}$, y existe una potencia de $\mathfrak{m}$ contenida en $\mathfrak{a}$, supongamos que $\mathfrak{m}^n \subseteq \mathfrak{a}$, entonces como $\mathfrak{a}/\mathfrak{m}^n \subseteq D/\mathfrak{m}^n$, y éste es un anillo local artiniano. Por ser $\dim_F(\frac{\mathfrak{m}/\mathfrak{m}^n}{\mathfrak{m}^2/\mathfrak{m}^n}) = 1$, tenemos que cada ideal de $D/\mathfrak{m}^n$ es una potencia del ideal maximal $\mathfrak{m}/\mathfrak{m}^n$. Aplicándolo a $\mathfrak{a}/\mathfrak{m}^n$, tenemos que $\mathfrak{a}$ es una potencia de $\mathfrak{m}$.

(e) $\Rightarrow$ (f). Tomamos $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, por la hipótesis tenemos que existe $n \in \mathbb{N}$ tal que $(x) = \mathfrak{m}^n$; entonces ha de ser $n = 1$ y por tanto $\mathfrak{m} = (x)$ es un ideal principal. Ahora, como cada ideal no nulo es una potencia del ideal maximal, tenemos el resultado.

(f) $\Rightarrow$ (a). Tenemos que (x) es el único ideal maximal. Dado $0 \neq r \in D$ un elemento no nulo, tenemos que $(r) = (x^n)$ para algún $n \in \mathbb{N}$. Para comprobar que este n es único, supongamos que $(x^n) = (x^n + 1)$, entonces existe $s \in D$ tal que $x^n = sx^{n+1}$, y como $x \neq 0$, tenemos $1 = sx$, esto es, x es una unidad, lo que es una contradicción. Este índice n lo representamos entonces por $n(r)$. Definimos ahora $v\colon K^* \to \mathbb{Z}$ mediante: $v(r/s) = n(r) - n(s)$; entonces v es una valoración sobre K con grupo de valoración $\mathbb{Z}$ y con anillo de valoración D, esto es, D es un dominio de valoración discreta.

(a) $\Rightarrow$ (g). Supongamos que D es un dominio de valoración discreta, entonces D no es un cuerpo, ya que para cada $n \in \mathbb{N}$ existe $x \in D$ verificando $v(x) = n$, luego si $n \neq 0$, entonces x no es una unidad. Por otro lado, sea $0 \neq \mathfrak{a} \subseteq D$ un ideal no nulo, llamamos $n = \min\{v(y) \mid 0 \neq y \in \mathfrak{a}\}$. Si $n = 0$, entonces $\mathfrak{a}$ contiene una unidad y tenemos $\mathfrak{a} = D$. Si $n \neq 0$, entonces sea $y \in \mathfrak{a}$ tal que $v(y) = n$, resulta que si $x \in \mathfrak{a}$, entonces $v(x) \geq v(y)$, luego $v(xy^{-1}) = v(x) - v(y) \geq 0$ y $xy^{-1} \in D$, esto es $x \in (y)$. Como consecuencia $\mathfrak{a} = (y)$ y entonces D es un dominio de ideales principales.

(g) $\Rightarrow$ (c). Es evidente.

(a+c) $\Rightarrow$ (h). Es evidente.

(h) $\Rightarrow$ (f). Basta ver que D es un dominio de ideales principales. Ya que los ideales de un anillo de valoración forman una cadena, cada ideal finitamente generado es principal, como D es noetheriano, resulta que cada ideal de D es principal. Otra vez por formar los ideales de D una cadena, resulta que D es un anillo local.

(a+c) $\Rightarrow$ (b). Es evidente.

(b) $\Rightarrow$ (c). Sea $\mathfrak{m}$ el ideal maximal de D, por el lema de Nakayama se tiene $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ para cada $n \in \mathbb{N}$. Sea $0 \neq a \in \mathfrak{m}$, ya que $\operatorname{rad}((a)) = \mathfrak{m}$, existe un exponente n tal que $\mathfrak{m}^n \subseteq (a)$; supongamos también que $\mathfrak{m}^{n-1} \nsubseteq (a)$. Entonces existe $b \in \mathfrak{m}^{n-1} \setminus (a)$; definimos $x = a/b \in K$. Ya que $b \notin (a)$, resulta que $x^{-1} \notin D$, como consecuencia x^{-1} no es entero sobre D, entonces $x^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$, ya que si $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, entonces $\mathfrak{m}$ sería un $D[x^{-1}]$–módulo fiel finitamente generado como D–módulo y entonces x^{-1} sería entero sobre D. Entonces, ya que se tiene $x^{-1}\mathfrak{m} \subseteq D$, resulta que $x^{-1}\mathfrak{m} = D$ y como consecuencia $\mathfrak{m} = (x)$. □

Corolario. 52.12.
Sea A un dominio noetheriano íntegramente cerrado y $\mathfrak{p}$ un ideal primo no nulo minimal de A. El localizado $A_\mathfrak{p}$ es un anillo de valoración discreta.

Ejemplo. 52.13.
Dado un dominio de ideales principales A y $\mathfrak{p} = (p)$ un ideal primo no nulo, entonces por el Corolario anterior $A_\mathfrak{p}$ es un dominio de valoración discreta. Este ejemplo generaliza los ejemplos (52.3.), (52.4.). En este caso la valoración, definida sobre K, el cuerpo de fracciones de A y de $A_\mathfrak{p}$, es $v_p : K^* \longrightarrow \mathbb{Z}$, definida por $v_p(p^s u) = s$.

53. Ideales fraccionarios

Sea D un dominio de integridad con cuerpo de fracciones K. Un **ideal fraccionario** de D es un D–submódulo no nulo $\mathfrak{b}$ de K para el que existe $0 \neq d \in D$ tal que $d\mathfrak{b} \subseteq D$.

Ejemplos. 53.1.

(1) Todo ideal no nulo de D es un ideal fraccionario de D. (En este contexto los ideales no nulos de D se suelen llamar **ideales enteros** de D.)

(2) Para cada elemento no nulo $k \in K$ se tiene que kD es un ideal fraccionario de D. Además, cada ideal fraccionario de D es de la forma $k\mathfrak{a}$, siendo $0 \neq k \in K$, y $0 \neq \mathfrak{a} \subseteq D$, un ideal entero de D.

(3) Si D es noetheriano los ideales fraccionarios de D son exactamente los D–submódulos no nulos finitamente generados de K.

Dada una familia de ideales fraccionarios $\{\mathfrak{b}_j \mid j \in J\}$, su intersección, si es no nula, es un ideal fraccionario. Para la suma no ocurre lo mismo; en este caso tenemos que restringir a sumas finitas: la suma finita de ideales fraccionarios es un ideal fraccionario. También el producto (finito) de ideales fraccionarios es un ideal fraccionario. Además el producto de ideales fraccionarios es distributivo con respecto a la suma, esto es,

$$\mathfrak{b}(\mathfrak{c}_1 + \mathfrak{c}_2) = \mathfrak{b}\mathfrak{c}_1 + \mathfrak{b}\mathfrak{c}_2.$$

para $\mathfrak{b}$, $\mathfrak{c}_1$ y $\mathfrak{c}_2$ ideales fraccionarios de D.

Para cada ideal fraccionario $\mathfrak{b}$ de D definimos el **inverso** de $\mathfrak{b}$ como $(D : \mathfrak{b}) = \{k \in K \mid k\mathfrak{b} \subseteq D\}$. El ideal fraccionario $(D : \mathfrak{b})$ se suele representar también por $\mathfrak{b}^{-1}$. Observa que se tiene $\mathfrak{b}(D : \mathfrak{b}) \subseteq D$. Un ideal fraccionario $\mathfrak{b}$ de D se llama **invertible** si $\mathfrak{b}(D : \mathfrak{b}) = D$.

Los ideales invertibles verifican propiedades de interés.

Proposición. 53.2.
Sea D un dominio de integridad, se verifica:

(1) Todo ideal fraccionario principal es invertible;
(2) Todo ideal fraccionario invertible es finitamente generado.

DEMOSTRACIÓN. (1). Es inmediato.

(2). Si $\mathfrak{b}$ es un ideal fraccionario invertible, entonces $1 = b_1c_1 + \cdots + b_tc_t$ para $b_1, \ldots, b_t \in \mathfrak{b}$ y $c_1, \ldots, c_t \in (D : \mathfrak{b})$, entonces $\{b_1, \ldots, b_t\}$ es un sistema finito de generadores de $\mathfrak{b}$. □

Proposición. 53.3.
Sea $\mathfrak{a}$ un ideal fraccionario de D. Se verifica:

(1) $\mathfrak{a}^{-1} = (D : \mathfrak{a})$ es un ideal fraccionario de D.

(2) $\mathfrak{a}$ *es invertible si, y sólo si,* $\mathfrak{a}\mathfrak{a}^{-1} = D$
(3) *Si* $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ *y* $\mathfrak{a}$ *es un ideal invertible, entonces* $\mathfrak{b} = \mathfrak{c}$.
(4) *El producto* $\mathfrak{a}_1 \cdots \mathfrak{a}_t$ *es un ideal invertible si, y sólo si, cada* $\mathfrak{a}_i$ *es un ideal invertible. En ese caso se verifica* $(\mathfrak{a}_1 \cdots \mathfrak{a}_t)^{-1} = \mathfrak{a}_1^{-1} \cdots \mathfrak{a}_t^{-1}$.

DEMOSTRACIÓN. (1). Es claro que $\mathfrak{a}^{-1}$ es un D–submódulo de K. Para ver que es un ideal fraccionario, tomamos $a \in \mathfrak{a} \cap D$, entonces $a\mathfrak{a}^{-1} \subseteq D$.
(2). Si existe un ideal fraccionario $\mathfrak{b}$ tal que $\mathfrak{a}\mathfrak{b} = D$, entonces se tiene $\mathfrak{a}^{-1} = D\mathfrak{a}^{-1} = \mathfrak{b}\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{b}D = \mathfrak{b}$.
(3). Basta considerar la siguiente cadena de igualdades: $\mathfrak{b} = D\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{b} = \mathfrak{a}^{-1}\mathfrak{a}\mathfrak{c} = D\mathfrak{c} = \mathfrak{c}$.
(4). La condición necesaria es evidente, ya que $(\mathfrak{a}_1 \cdots \mathfrak{a}_t)\mathfrak{a}_1^{-1} \cdots \mathfrak{a}_t^{-1} = D$. Para la condición suficiente, si $\mathfrak{a}_1 \cdots \mathfrak{a}_t$ es invertible, existe un ideal fraccionario $\mathfrak{b}$ tal que $(\mathfrak{a}_1 \cdots \mathfrak{a}_t)\mathfrak{b} = D$, y se verifica $\mathfrak{a}_1(\mathfrak{a}_2 \cdots \mathfrak{a}_t)\mathfrak{b} = D$, luego $\mathfrak{a}_1$ es invertible; igual sucede con cada $\mathfrak{a}_i$. □

Proposición. 53.4.
Sean $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m$ *ideales primos de* D *verificando:*
(1) $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$ *y*
(2) *Cada* $\mathfrak{p}_i$ *es invertible.*

Entonces $n = m$, *y salvo una permutación se tiene* $\mathfrak{p}_i = \mathfrak{q}_i$ *para cada índice* i.

DEMOSTRACIÓN. Hagamos la demostración por inducción sobre n. Si $n = 1$, entonces $\mathfrak{p}_1 = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, y existe j tal que $\mathfrak{q}_j = \mathfrak{p}_1$; supongamos por simplicidad que $j = 1$, entonces tenemos $D = \mathfrak{p}_1^{-1}\mathfrak{p}_1 = \mathfrak{p}_1^{-1}\mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_m = \mathfrak{q}_2 \cdots \mathfrak{q}_m$, entonces necesariamente $m = 1$ y el resultado es cierto. Supongamos que sea cierto el resultado para $n-1$. Supongamos que $\mathfrak{p}_1$ es minimal entre los $\mathfrak{p}_i$, entonces $\mathfrak{q}_1 \cdots \mathfrak{q}_m = \mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{p}_1$, y existe j tal que $\mathfrak{q}_j \subseteq \mathfrak{p}_1$, supongamos que $j = 1$. Tenemos también $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m \subseteq \mathfrak{q}_1$, luego existe i tal que $\mathfrak{p}_i \subseteq \mathfrak{q}_1 \subseteq \mathfrak{p}_1$, luego por la minimalidad de $\mathfrak{p}_1$ resulta que $\mathfrak{p}_1 = \mathfrak{q}_1$, y por ser $\mathfrak{p}_1$ invertible tenemos $\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m$. Aplicando ahora la hipótesis de inducción tenemos el resultado. □

Proposición. 53.5.
Dado un dominio de integridad D *se verifica:*
(1) *El conjunto* $\mathcal{I}(D)$ *de los ideales fraccionarios invertibles tiene estructura de grupo abeliano para la multiplicación de ideales.*
(2) *Los ideales fraccionarios principales no nulos forman un subgrupo,* $\mathcal{P}(D)$, *del grupo* $\mathcal{I}(D)$.

Al grupo cociente $\mathcal{I}(D)/\mathcal{P}(D)$ lo llamamos el **grupo de clases** de D. Lo representamos por $\mathrm{Cl}(D)$, y su orden lo llamamos el **número de clases** de D. Observa que si D es un DIP, entonces el grupo de clases es trivial, por tanto su número de clases es igual a uno. Se utiliza pues el número de clases como una medida de cuanto se aleja un dominio de integridad de ser un DIP.

Veamos cómo podemos utilizar los ideales invertibles para caracterizar dominios de valoración discreta.

Proposición. 53.6.
Sea D un dominio local que no es un cuerpo. Son equivalentes:

(a) D es un dominio de valoración discreta.
(b) Cada ideal fraccionario de D es invertible.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si D es un dominio de valoración discreta, todo ideal es de la forma t^sD, con $s \in \mathbb{N}$ y t un parámetro de uniformización, entonces todo ideal fraccionario es principal, y por tanto invertible.

(b) $\Rightarrow$ (a). Si todo ideal fraccionario no nulo es invertible, entonces todo ideal no nulo es finitamente generado y por tanto D es un anillo noetheriano.

Sea $\mathfrak{m}$ el ideal maximal de D. Si $\mathfrak{m} = \mathfrak{m}^2$, por el Lema de Nakayama, se tiene $\mathfrak{m} = 0$, y entonces D es un cuerpo, lo que es una contradicción. Tenemos pues $\mathfrak{m} \neq \mathfrak{m}^2$.

Sea $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. Si $t\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, entonces $t \in \mathfrak{m}^2$, lo que es una contradicción, por tanto $t\mathfrak{m}^{-1} = D$ y resulta que $\mathfrak{m} = tD$ es un ideal principal. Veamos que cada ideal de D es una potencia de $\mathfrak{m}$. Llamamos $\Gamma = \{\mathfrak{a} \mid\ 0 \neq \mathfrak{a} \text{ no es potencia de } \mathfrak{m}\}$. Por ser D noetheriano, existe un elemento maximal $\mathfrak{a}$ en Γ. Se tiene $\mathfrak{a} \subseteq m$ y $\mathfrak{a}\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = D$. Como $\mathfrak{a} \subseteq \mathfrak{a}\mathfrak{m}^{-1}$ se tiene $\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1}$, y por tanto $\mathfrak{a}\mathfrak{m} = \mathfrak{a}$, y por el Lema de Nakayama resulta $\mathfrak{a} = 0$, lo que es una contradicción, o $\mathfrak{a} \subsetneq \mathfrak{a}\mathfrak{m}^{-1}$, y por tanto $\mathfrak{a}\mathfrak{m}^{-1}$ es una potencia de $\mathfrak{m}$, lo que implica que $\mathfrak{a}$es una potencia de $\mathfrak{m}$, lo que es una contradicción. Por tanto $\Gamma = \varnothing$ y cada ideal no nulo de A es una potencia de $\mathfrak{m}$. Por tanto D es un dominio de valoración discreta. □

Ejercicio. 53.7.
Sea D un dominio de integridad con cuerpo de fracciones K y sea $\mathfrak{p}$ un ideal primo no nulo de D. Se verifica:

(1) Para todo ideal fraccionario $\mathfrak{a}$ de D el módulo $\mathfrak{a}D_\mathfrak{p}$ es un ideal fraccionario de $D_\mathfrak{p}$.
(2) Todo ideal fraccionario de $D_\mathfrak{p}$ es de la forma $\mathfrak{a}D_\mathfrak{p}$, con $\mathfrak{a}$ ideal fraccionario de D.
(3) Si $\mathfrak{a}$ es un ideal fraccionario finitamente generado, entonces $(\mathfrak{a}^{-1})_\mathfrak{p} = (\mathfrak{a}_\mathfrak{p})^{-1}$.

54. Dominios de Dedekind

Los dominios de integridad (no necesariamente locales) que verifican la propiedad de que todos los ideales fraccionarios son invertibles se llaman **dominios de Dedekind**. La Proposición (53.6.) prueba que los dominios de Dedekind locales son los dominios de valoración discreta. Se trata ahora de caracterizar los dominios de Dedekind siguiendo el Teorema (52.11.).

En lo que sigue D será un dominio de integridad y K su cuerpo de fracciones.

Teorema. 54.1.
Sea D un dominio de integridad que no es un cuerpo. Son equivalentes las siguientes condiciones:

(a) D es un dominio de Dedekind.
(b) D es un dominio noetheriano y para cada ideal primo no nulo $\mathfrak{p}$ el localizado $D_\mathfrak{p}$ es un dominio de valoración discreta.
(c) D es un dominio noetheriano íntegramente cerrado en el que cada ideal primo no nulo es maximal (= de dimensión uno).
(d) Todo ideal propio y no nulo $\mathfrak{a}$ es un producto finito de ideales primos (no necesariamente distintos); $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Como todo ideal fraccionario es invertible, resulta que todo ideal entero no nulo es finitamente generado, luego D es noetheriano. Por otro lado, para cada ideal primo $\mathfrak{p}$ el anillo local $D_\mathfrak{p}$ verifica que cada ideal fraccionario es invertible, luego $D_\mathfrak{p}$ es un dominio de valoración discreta.

(b) $\Rightarrow$ (c). Para cada ideal primo no nulo $\mathfrak{p}$ tenemos que $D_\mathfrak{p}$ es un dominio de valoración discreta, por lo tanto es íntegramente cerrado, y como la intersección de íntegramente cerrados lo es, basta ver que $D = \cap_{\mathfrak{p}\neq 0} D_\mathfrak{p}$; ver el Ejercicio (43.52.).

Para ver que cada ideal primo no nulo es maximal, sea $\mathfrak{p}$ un ideal primo no nulo y $\mathfrak{m}$ un ideal maximal tal que $\mathfrak{p} \subseteq \mathfrak{m}$. Como el localizado $D_\mathfrak{m}$ es un dominio de valoración discreta, tenemos que $\mathfrak{p}D_\mathfrak{m} = \mathfrak{m}D_\mathfrak{m}$, y por tanto $\mathfrak{p} = \mathfrak{m}$.

(c) $\Rightarrow$ (d). Dado un ideal no nulo $\mathfrak{a}$, consideramos una descomposición primaria minimal $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t$. Sea $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. Observa que los ideales $\mathfrak{p}_i$ son no nulos, ya que si $0 = \mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i) \supseteq \mathfrak{q}_i$, entonces $\mathfrak{q}_i = 0$.

Veamos que los $\mathfrak{q}_i$ son comaximales dos a dos. Si $\mathfrak{q}_1 + \mathfrak{q}_2 \neq D$, existe un ideal maximal $\mathfrak{m}$ tal que $\mathfrak{q}_1 + \mathfrak{q}_2 \subseteq \mathfrak{m}$. Como $\mathfrak{p}_i$ es el menor ideal primo que contiene a $\mathfrak{q}_i$, resulta $\mathfrak{p}_i \subseteq \mathfrak{m}$, y como cada ideal primo no nulo es maximal, resulta $\mathfrak{p}_1 = \mathfrak{m} = \mathfrak{p}_2$, lo que es una contradicción. Tenemos entonces $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t = \mathfrak{q}_1 \cdots \mathfrak{q}_t$.

Dado un ideal $\mathfrak{p}$-primario $\mathfrak{q}$, con $\mathfrak{p} \neq 0$, en el anillo local $D_\mathfrak{p}$ el ideal $\mathfrak{q}D_\mathfrak{p}$ es $\mathfrak{p}D_\mathfrak{p}$–primario, y como $D_\mathfrak{p}$ es un dominio de valoración discreta se tiene $\mathfrak{q}D_\mathfrak{p} = (\mathfrak{p}D_\mathfrak{p})^n$ para $n \in \mathbb{N}$. Entonces $\mathfrak{q} = \mathfrak{p}^n$, ya que ambos son $\mathfrak{p}$–primarios. Por tanto existen $n_1, \ldots, n_t \in \mathbb{N}$ tales que $\mathfrak{a} = \mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_t^{n_t}$.

(d) $\Rightarrow$ (a). (1) Primero probamos que cada factorización $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$, en la que los $\mathfrak{p}_i$ son ideales primos invertibles, es única.

Si tenemos dos factorizaciones $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_t = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$. Tomamos un índice j tal que $\mathfrak{p}'_j$ sea minimal en $\{\mathfrak{p}'_1, \ldots, \mathfrak{p}'_s\}$, se tiene $\mathfrak{p}_1 \cdots \mathfrak{p}_t = \mathfrak{p}'_j$, y existe $\mathfrak{p}_i$ tal que $\mathfrak{p}_i \subseteq \mathfrak{p}'_j$. Dado el índice i existe un índice h tal que $\mathfrak{p}'_h \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}'_j$; la minimalidad de $\mathfrak{p}'_j$ implica que $\mathfrak{p}_i = \mathfrak{p}'_j$; supongamos que $i = 1 = j$. Como $\mathfrak{p}_1$ es invertible resulta $\mathfrak{p}_2 \cdots \mathfrak{p}_t = \mathfrak{p}'_2 \cdots \mathfrak{p}'_s$, y por inducción llegamos a que $t = s$ y a que $\{\mathfrak{p}_2, \ldots, \mathfrak{p}_t\} = \{\mathfrak{p}'_2, \ldots, \mathfrak{p}'_s\}$.

(2) Si se verifica (d) todo ideal primo invertible es un ideal maximal.

Dado $\mathfrak{p}$ un ideal primo invertible, tomamos $a \notin \mathfrak{p}$ y escribimos $\mathfrak{p} + aD = \mathfrak{p}_1 \cdots \mathfrak{p}_t$. Hacemos la misma construcción para $\mathfrak{p} + a^2D$; teniendo $\mathfrak{p} + a^2D = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s$. Pasando al cociente $D/\mathfrak{p}$ tenemos las expresiones:

$$a(D/\mathfrak{p}) = (\mathfrak{p}_1/\mathfrak{p}) \cdots (\mathfrak{p}_t/\mathfrak{p}),$$
$$a^2(D/\mathfrak{p}) = (\mathfrak{p}'_1/\mathfrak{p}) \cdots (\mathfrak{p}'_s/\mathfrak{p}),$$

y por tanto

$$(\mathfrak{p}_1/\mathfrak{p})^2 \cdots (\mathfrak{p}_t/\mathfrak{p})^2 = a^2(D/\mathfrak{p}) = (\mathfrak{p}'_1/\mathfrak{p}) \cdots (\mathfrak{p}'_s/\mathfrak{p})$$

es una factorización del ideal $a^2(D/\mathfrak{p})$ en ideales primos invertibles. Por (1) esta descomposición es única, y por tanto las colecciones $\mathfrak{p}_1, \mathfrak{p}_1, \ldots, \mathfrak{p}_t, \mathfrak{p}_t$ y $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_s$ son iguales (salvo en el orden). Tenemos entonces:

$$\mathfrak{p} \subseteq \mathfrak{p} + a^2D = \mathfrak{p}'_1 \cdots \mathfrak{p}'_s = \mathfrak{p}_1\mathfrak{p}_1 \cdots \mathfrak{p}_t\mathfrak{p}_t = (\mathfrak{p} + aD)^2 \subseteq \mathfrak{p}^2 + aD.$$

En particular cada elemento $x \in \mathfrak{p}$ se escribe en la forma $x = y + ad$, con $y \in \mathfrak{p}^2$ y $d \in D$, luego $ad = x - y \in \mathfrak{p}$ y se tiene $d \in \mathfrak{p}$, esto es, $x \in \mathfrak{p}^2 + a\mathfrak{p}$, y se tiene $\mathfrak{p}^2 + a\mathfrak{p} \subseteq \mathfrak{p} \subseteq \mathfrak{p}^2 + a\mathfrak{p}$, luego $\mathfrak{p} = \mathfrak{p}^2 + a\mathfrak{p}$. Por ser $\mathfrak{p}$ invertible, se tiene $D = \mathfrak{p} + aD$ y por tanto $\mathfrak{p}$ es un ideal maximal.

(3) Si se verifica (d) los ideales primo no nulos son invertibles.

Si $\mathfrak{p}$ es un ideal primo no nulo, tomamos $0 \neq a \in \mathfrak{p}$; existen ideales primos tales que $aD = \mathfrak{p}_1 \cdots \mathfrak{p}_t \subseteq \mathfrak{p}$, luego todos los ideales $\mathfrak{p}_i$ son invertibles, y aplicando (2) son maximales, y como algún $\mathfrak{p}_i \subseteq \mathfrak{p}$, tenemos que $\mathfrak{p}$ es maximal.

Para probar la implicación, dado un ideal fraccionario $\mathfrak{a}$, podemos suponer que es entero, consideramos una factorización $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_t$. Por (3) cada ideal $\mathfrak{p}_i$ es invertible, y por tanto $\mathfrak{a}$ es un ideal invertible. □

Como consecuencia del Teorema, dado un ideal no nulo $\mathfrak{a}$ con factorización $\mathfrak{p}_1 \cdots \mathfrak{p}_t$, los ideales $\mathfrak{p}_i$ están determinados de forma única, salvo en el orden, y en consecuencia en dominios de Dedekind se tiene un teorema de unicidad de la descomposición de ideales no nulos como producto de ideales primos.

Ejemplos y construcciones de dominios de Dedekind

Proposición. 54.2.
Si D es un dominio de Dedekind y $\Sigma \subseteq D$ es un subconjunto multiplicativo, entonces $\Sigma^{-1}D$ es un dominio de Dedekind.

DEMOSTRACIÓN. Ver Ejercicio (56.11.). □

Proposición. 54.3.
Todo dominio de ideales principales es un dominio de Dedekind.

El recíproco no es cierto.

Ejemplo. 54.4.
Vamos a ver que el anillo $\mathbb{Z}[\sqrt{-5}]$ es un dominio de Dedekind y no es un dominio de ideales principales, ya que no es un dominio de factorización única.

Para estudiar este ejemplo vamos a hacer previamente el siguiente resultado.

Proposición. 54.5.
Sea D un dominio de Dedekind con cuerpo de fracciones K y L/K una extensión finita separable de cuerpos. Si E es la clausura entera de D en L, entonces E es un dominio de Dedekind.
Como consecuencia, para cada cuerpo de números algebraicos el anillo de enteros (la clausura entera de $\mathbb{Z}$) es un dominio de Dedekind.

DEMOSTRACIÓN. (1) Sea A un dominio normal con cuerpo de fracciones K y L/K una extensión finita separable. Si B es la clausura entera de A en L, entonces existe una base $y_1,\ldots,y_t$ de L sobre K tal que $B \subseteq \sum_{i=1}^{t} y_i$.
Dado $x \in L$, como x es algebraico sobre K, existe $a_nx^n+\cdots+a_1x+a_0 = 0$ con $a_i \in A$, $a_n \neq 0$. Entonces $(a_nx)^n + a_{n-1}(a_nx^n)^{n-1} + \cdots + a_1a_n^{n-2}(a_nx) + a_0a_n^{n-1} = 0$ y por tanto a_nx es entero sobre A, esto es, $a_nx \in B$. Por lo tanto dada una base de L sobre K podemos encontrar múltiplos de cada elemento que pertenezcan a B, esto es, podemos suponer que la base está contenida en B.
Por ser L/K separable la traza define una forma bilineal no degenerada; $T(x,y) = T(xy)$, y existe dada una base $\{x_1,\ldots,x_t\}$ de L en B existe una base dual $\{y_1,\ldots,y_t\}$ tal que $T(x_iy_j) = \delta_{i,j}$. Dado $b \in B$ existe una combinación $b = \sum_{i=1}^{t} k_iy_i$ con $k_i \in K$. Para cada índice i se tiene $bx_i \in B$, ya que es el producto de dos elementos de B, además la traza de un elemento de B pertenece a A, ver la Proposición (35.19.), en particular

$$k_j = \sum_{i=1}^{t} k_i\delta_{i,j} = \sum_{i=1}^{t} k_iT(y_ix_j) = T((\sum_{i=1}^{t} k_iy_i)x_j) = T(bx_j) \in B.$$

Por lo tanto $b \in \sum_{i=1}^{t} Ay_i$. Aplicamos este resultado al dominio de Dedekind D.
(2) Por ser D noetheriano, se tiene $E \subseteq \sum_{i=1}^{t} Dy_i$ es un D–módulo noetheriano, y por tanto un anillo noetheriano.
(3) Tenemos que E es íntegramente cerrado en L, luego es un dominio normal.
(4) Falta ver que cada ideal primo no nulo de D es maximal para tener que E es un dominio de Dedekind. Dado un ideal primo no nulo $\mathfrak{p}$ de E, se tiene que $\mathfrak{p} \cap D$ es un ideal primo no nulo, y por tanto maximal, y por el Corolario (35.13.) tenemos que $\mathfrak{p}$ es un ideal maximal. □

Para completar el Ejemplo (54.4.) basta ver que $\mathbb{Z}[\sqrt{-5}]$ es la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{-5}]$.

Proposición. 54.6.
Dada la extensión $\mathbb{Q}[\sqrt{d}]$, con d libre de cuadrados, la clausura entera E de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{d}]$ es:

$$E = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & \text{si } d \equiv 1 \pmod 4 \text{ y} \\ \mathbb{Z}[\sqrt{d}] & \text{en otro caso.} \end{cases}$$

DEMOSTRACIÓN. Dado $x \in E$ podemos escribir $x = \frac{a+b\sqrt{d}}{m}$ con $\text{m.c.d.}\{a,b,m\} = 1$. Tenemos que x es raíz del polinomio $X^2 - 2\frac{a}{m}X + \frac{a^2-db^2}{m^2}$. Si $b = 0$, y como se tiene $X^2 - 2\frac{a}{m}X + \frac{a^2-db^2}{m^2} = \left(X - \frac{a}{m}\right)^2$, entonces x es raíz de $X - \frac{a}{m}$, esto es, $x = \frac{a}{m} \in \mathbb{Q}$, y como es entero sobre $\mathbb{Z}$, entonces $x \in \mathbb{Z}$. Supongamos que $b \neq 0$, entonces x es raíz de $X^2 - 2\frac{a}{m}X + \frac{a^2-db^2}{m^2}$, y éste es irreducible, por tanto sus coeficientes pertenecen a $\mathbb{Z}$.
Llamamos $h = \text{m.c.d.}\{a,m\}$, entonces $h^2 \mid db^2$, y como $\text{m.c.d.}\{h,b\} = 1$, entonces $h^2 \mid d$, pero d es libre de cuadrados, luego $h = 1$.
Como $\frac{2a}{m} \in \mathbb{Z}$, entonces $m \mid 2a$, y se tiene $m \mid 2$.
Si $m = 2$ entonces a es impar, y de $\frac{a^2-db^2}{m^2} \in \mathbb{Z}$ se deduce $4 \mid a^2 - db^2$, esto es, b es impar y $d \equiv 1 \pmod 4$, entonces $E = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, ya que

$$\frac{a+b\sqrt{d}}{2} = \frac{a-b}{2} + b\frac{1+\sqrt{d}}{2}.$$

Si $m = 1$, entonces $E = \mathbb{Z}[\sqrt{d}]$. □

En particular, como $-5 \not\equiv 1 \pmod 4$, tenemos que la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{-5}]$ es $\mathbb{Z}[\sqrt{-5}]$.

Ejemplo. 54.7.
Observa que la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}[\sqrt{5}]$, según este resultado es: $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$

Ejercicio. 54.8.
Determina un polinomio mónico con coeficientes en $\mathbb{Z}$ del que el elemento $\frac{1+\sqrt{5}}{2}$ sea raíz.

SOLUCIÓN. Un polinomio es: $X^2 - X - 1$. □

Surge ahora el problema de describir los ideales de los dominios de Dedekind E que son clausuras enteras de $\mathbb{Z}$ en cuerpos de números, y también estudiar si amén de ser dominios de Dedekind verifican alguna otra propiedad adicional.

Nota. 54.9.
El anillo de enteros de $\mathbb{Q}[\sqrt{d}]$ es un DIP para los siguientes valores de d, libre de cuadrados y menor que 0: $d = -1, -2, -3, -7, -11, -18, -43, -67, -163$. Por otro lado C. Gauss conjeturó que hay infinitos valores de d libre de cuadrados y mayor que 0 para los cuales el anillo de enteros es un DIP (¡sin probar!).

Teoría de divisibilidad de ideales en dominios de Dedekind

Dado un dominio de integridad D y dos ideales $\mathfrak{a}$ y $\mathfrak{b}$, decimos que $\mathfrak{a}$ **divide** a $\mathfrak{b}$, o que $\mathfrak{b}$ es **divisible** por $\mathfrak{a}$, si existe un ideal $\mathfrak{c}$ tal que $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.

Lema. 54.10.
En un dominio de integridad un ideal $\mathfrak{a}$ divide a otro ideal $\mathfrak{b}$ si $\mathfrak{b} \subseteq \mathfrak{a}$.

Corolario. 54.11.
En un dominio de Dedekind para dos ideales no nulos $\mathfrak{a}$ y $\mathfrak{b}$ se verifica que $\mathfrak{a}$ divide a $\mathfrak{b}$ si y solo si $\mathfrak{b} \subseteq \mathfrak{a}$.

En la forma obvia podemos definir el **máximo común divisor** de dos ideales $\mathfrak{a}$ y $\mathfrak{b}$, ideal al que vamos a representar por $(\mathfrak{a}, \mathfrak{b})$.

Proposición. 54.12.
Sea D un dominio de Dedekind y $\mathfrak{a}$, $\mathfrak{b}$ ideales no nulos con factorización en producto de ideales primos distintos: $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$ y $\mathfrak{b} = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_t^{b_t}$, con $a_i, b_i \in \mathbb{N}$. Se verifica:
(1) $\mathfrak{a} \subseteq \mathfrak{b}$ si y solo si $a_i \geq b_i$ para cada índice $i = 1, \ldots, t$.
(2) $\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_t^{c_t}$, siendo $c_i = min\{a_i, b_i\}$ para $i = 1, \ldots, t$.
(3) $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_t^{d_t}$, siendo $d_i = max\{a_i, b_i\}$ para $i = 1, \ldots, t$.

Proposición. 54.13.
Sea D un dominio de Dedekind y $\mathfrak{a}$ un ideal no nulo con factorización en producto de ideales primos distintos $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}$. Existe un isomorfismo de anillos

$$\frac{D}{\mathfrak{a}} = \frac{D}{\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t}} \cong \left(\frac{D}{\mathfrak{p}_1^{a_1}}\right) \times \cdots \times \left(\frac{D}{\mathfrak{p}_t^{a_t}}\right).$$

Aritmética de los ideales en dominios de Dedekind

Proposición. 54.14.
Sea D un dominio de Dedekind y $\mathfrak{a}$ un ideal no nulo. Se verifica:
(1) Existe un ideal $\mathfrak{b}$ tal que $\mathfrak{a}+\mathfrak{b}=D$ y $\mathfrak{a}\mathfrak{b}$ es un ideal principal.
(2) Todo ideal del anillo cociente $D/\mathfrak{a}$ es un ideal principal.

DEMOSTRACIÓN. (1). Sea $\mathfrak{a}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$ la factorización en producto de ideales primos distintos de $\mathfrak{a}$. Definimos dos ideales:

$$\begin{aligned}\mathfrak{a}_0&=\mathfrak{a}\mathfrak{p}_1\cdots\mathfrak{p}_t,\\ \mathfrak{a}_i&=\mathfrak{a}\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_t.\end{aligned}$$

Se verifica $\mathfrak{a}_0\subsetneq\mathfrak{a}_i\subsetneq\mathfrak{a}$. Para cada índice i tomamos un elemento $a_i\in\mathfrak{a}_i\setminus\mathfrak{a}_0$ y definimos $a=a_1+\cdots+a_t$. Como $a\in\mathfrak{p}_i^{e_i}\setminus\mathfrak{p}_i^{e_i+1}$, la factorización de aD com producto de ideales primos distintos es: $aD=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}\mathfrak{p}_{t+1}^{e_{t+1}}\cdots\mathfrak{p}_{t+s}^{e_{t+s}}$. El ideal que andamos buscado es el ideal $\mathfrak{b}=\mathfrak{p}_{t+1}^{e_{t+1}}\cdots\mathfrak{p}_{t+s}^{e_{t+s}}$.
(2). Primero probamos que si $\mathfrak{f}$ es un ideal fraccionario y $\mathfrak{g}$ es un ideal entero, existe un $a\in\mathfrak{f}$ tal que $\mathfrak{f}^{-1}a+\mathfrak{g}=D$.
Si $\mathfrak{g}=\mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_t^{e_t}$, definimos

$$\begin{aligned}\mathfrak{f}_0&=\mathfrak{f}\mathfrak{p}_1\cdots\mathfrak{p}_t,\\ \mathfrak{f}_i&=\mathfrak{f}\mathfrak{p}_1\cdots\mathfrak{p}_{i-1}\mathfrak{p}_{i+1}\cdots\mathfrak{p}_t.\end{aligned}$$

Se verifica $\mathfrak{f}_0\subsetneq\mathfrak{f}_i\subsetneq\mathfrak{f}$. Para cada índice i tomamos un elemento $a_i\in\mathfrak{f}_i\setminus\mathfrak{f}_0$ y definimos $a=a_1+\cdots+a_t$. Se verifica

$$\begin{aligned}&\mathfrak{f}^{-1}a\subseteq D,\\ &\mathfrak{f}^{-1}a\nsubseteq\mathfrak{p}_i,\ \text{ para cada índice } i,\end{aligned}$$

entonces $\mathfrak{p}_i\nmid\mathfrak{f}^{-1}a$ y $\mathfrak{f}^{-1}a+\mathfrak{g}=\mathrm{m.c.d.}\{\mathfrak{f}^{-1}a,\mathfrak{g}\}=D$.
Para hacer la demostración, sea $\mathfrak{b}\supseteq\mathfrak{a}$ un ideal. Tomamos $\mathfrak{f}=\mathfrak{b}$ y $\mathfrak{g}=\mathfrak{b}^{-1}\mathfrak{a}$. Observa que de $\mathfrak{a}\subseteq\mathfrak{b}$ se deduce que $\mathfrak{g}=\mathfrak{b}^{-1}\mathfrak{a}\subseteq\mathfrak{b}^{-1}\mathfrak{b}=D$. Aplicado el resultado del párrafo anterior existe $a\in\mathfrak{b}$ tal que $\mathfrak{b}^{-1}a+\mathfrak{b}^{-1}\mathfrak{a}=D$; multiplicando por $\mathfrak{b}$ se tiene $aD+\mathfrak{a}=\mathfrak{b}$, y tenemos el resultado. □

Corolario. 54.15.
Sea D un dominio de Dedekind y $\mathfrak{a}$ un ideal no nulo. Para todo elemento no nulo $0\neq a\in\mathfrak{a}$ existe un elemento $b\in\mathfrak{a}$ tal que $\mathfrak{a}=aD+bD$.

DEMOSTRACIÓN. Basta tomar $\mathfrak{b}=\mathfrak{a}$ y $\mathfrak{a}=aD$ en el punto (2) de la Proposición (54.14.). □

En realidad la propiedad de que los ideales no nulos estén generados por dos elementos va a caracterizar a los dominios de Dedekind.

Proposición. 54.16.
Sea D un dominio de integridad que verifica la propiedad: "para cada ideal no nulo $\mathfrak{a}$ y cada elemento no nulo $a \in \mathfrak{a}$ existe $b \in \mathfrak{a}$ tal que $\mathfrak{a} = aD + bD$", entonces D es un dominio de Dedekind.

DEMOSTRACIÓN. Veamos el caso local. Si D es un dominio local con ideal maximal $\mathfrak{m}$, para cada ideal no nulo $\mathfrak{a}$, tomando $0 \neq a \in \mathfrak{m}\mathfrak{a}$ existe $b \in \mathfrak{a}$ tal que $\mathfrak{a} = aD + bD$; en particular $\mathfrak{a} = \mathfrak{m}\mathfrak{a} + bD$. Aplicando el Lema de Nakayama se tiene $\mathfrak{a} = bD$, por lo tanto todo ideal de D es principal y D es un dominio de valoración discreta.

En el caso general, como cada ideal está generado por al menos dos elementos, resulta que D es un dominio noetheriano. Si $\mathfrak{p}$ es un ideal primo no nulo de D, también el anillo $D_{\mathfrak{p}}$ verifica la propiedad del enunciado, luego $D_{\mathfrak{p}}$ es un dominio de valoración, y por tanto D es un dominio de Dedekind. □

Proposición. 54.17.
Sea D un dominio de Dedekind. Son equivalentes las siguientes condiciones:

(a) D es un dominio de factorización única.
(b) D es un dominio de ideales principales (su número de clase es igual a uno).

DEMOSTRACIÓN. Sea D un dominio de Dedekind que es un dominio de factorización única y sea $\mathfrak{p}$ un ideal primo no nulo, entonces $\mathfrak{p}$ está generado por dos elementos, sea $\mathfrak{p} = aD + bD$. Consideramos una factorización en producto de elementos primos de a; $a = p_1 \cdots p_s$. Es claro que uno de los p_i, por ejemplo p_1, pertenece a $\mathfrak{p}$, entonces $p_1D \subseteq \mathfrak{p}$, y como cada ideal primo no nulo es maximal tenemos $\mathfrak{p} = pD$; esto es, todo ideal primo es un ideal principal. Como todo ideal no nulo es un producto de ideales primos, y cada ideal primo no nulo es principal, tenemos que cada ideal no nulo es un ideal principal. □

Este resultado sobre ideales primos no es válido para anillos de enteros algebraicos, ya que no todo anillo de enteros algebraicos es un dominio de factorización única. Sin embargo en éstos tenemos un resultado de cierto interés.

Proposición. 54.18.
Sea D un anillo de enteros algebraicos (la clausura entera de $\mathbb{Z}$ en una extensión finita de $\mathbb{Q}$), entonces cada ideal primo no nulo $\mathfrak{p}$ de D es de la forma $\mathfrak{p} = pD + aD$, siendo $p \in \mathbb{Z}$ un entero primo.

DEMOSTRACIÓN. Basta considerar la intersección de $\mathfrak{p}$ con $\mathbb{Z}$ para determinar el elemento primo p. □

Ejercicio. 54.19.
Sea D un dominio de Dedekind, para cada ideal primo no nulo $\mathfrak{p}$ de D, para cada $a \notin \mathfrak{p}$ se verifica $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}a$.

SOLUCIÓN. Como $\mathfrak{p}$ es primo no nulo entonces es maximal, y se tiene $\mathfrak{p} + Da = D$. Multiplicando por $\mathfrak{p}$ tenemos $\mathfrak{p} = \mathfrak{p}^2 + \mathfrak{p}a$. □

55. Módulos proyectivos

Un A–módulo P se llama **proyectivo** si el funtor $\mathrm{Hom}_A(P,-)$ es exacto, esto es, si para cada sucesión exacta corta $0 \to M' \to M \to M'' \to 0$, la sucesión $0 \to \mathrm{Hom}_A(P,M') \to \mathrm{Hom}_A(P,M) \to \mathrm{Hom}_A(P,M'') \to 0$ es exacta.

Proposición. 55.1.
Para cada A–módulo P son equivalentes:

(a) P es proyectivo.
(b) Cada diagrama con filas exactas

$$\begin{array}{ccccc} & & P & & \\ & \swarrow & \downarrow & & \\ M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

se puede completar a un diagrama conmutativo.
(c) P es un sumando directo de un A–módulo libre.
(d) Toda sucesión exacta corta $0 \to M' \to M \to P \to 0$ escinde.

Lema. 55.2.
Son ciertos los siguientes enunciados:

(1) Cada sumando directo de un módulo proyectivo es proyectivo.
(2) La suma directa de módulos proyectivos es proyectivo.
(3) En una sucesión exacta $0 \to P' \to P \to P'' \to 0$, si P' y P'' son proyectivos, entonces P es proyectivo.

Módulos proyectivos finitamente generados

Proposición. 55.3.
Un A–módulo proyectivo P es finitamente generado si, y sólo si, es un sumando directo de A^n para un cierto n (esto es, de un A–módulo libre finitamente generado).

Observación. 55.4.
(1) Para anillo conmutativo A se verifica que si $A^n \subseteq A^m$, entonces $n \leq m$.

(2) Si F es un módulo libre finitamente generado, existe un único $n \in \mathbb{N}$ tal que $F \cong A^n$. Llamamos a n el **rango** de F.

Podemos caracterizar fácilmente los dominios D para los que cada submódulo de un módulo libre finitamente generado es libre.

Proposición. 55.5.
Si D es un DIP entonces todo submódulo de un módulo libre finitamente generado es un módulo libre. En particular, todo módulo proyectivo finitamente generado es libre.

DEMOSTRACIÓN. Sea $M \subseteq D^n$. Si $n = 1$, entonces M es un ideal principal, y por tanto libre de rango uno, ya que D es un dominio. Supongamos que para cada $M \subseteq D^m$, con $m < n$, se tiene que M es libre, y supongamos que $M \subseteq D^n$. Consideramos la proyección $p : D^n \to D$ definida $p(a_1, \ldots, a_n) = a_n$. Si $p(M) = 0$, entonces $M \subseteq \operatorname{Ker}(p) \cong D^{n-1}$, y M es libre. Si $p(M) \neq 0$, consideramos el siguiente diagrama conmutativo con filas son exactas.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D^{n-1} \cap M & \longrightarrow & M & \longrightarrow & p(M) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D^{n-1} & \longrightarrow & D^n & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

Por la hipótesis $D^{n-1} \cap M$ y $p(M)$ son libres, y por tanto M es libre.
Para la segunda parte basta tener en cuenta que todo módulo proyectivo finitamente generado es un submódulo de un módulo libre finitamente generado. □

Una consecuencia de este resultado es la caracterización de los DIP en términos de módulos libres.

Teorema. 55.6.
Sea D un dominio. Son equivalentes:
(a) D es un DIP.
(b) Cada submódulo de módulo libre finitamente generado es libre.

Vamos ahora a determinar los dominios D para los que cada submódulo de un módulo libre finitamente generado, D^n, es proyectivo.

Un A–módulo E se llama **inyectivo** si podemos completar cualquier diagrama con fila exacta

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \longrightarrow & M \\ & & \downarrow & \swarrow & \\ & & E & & \end{array}$$

Equivalentemente, para cada sucesión exacta corta $0 \to M' \to M \to M'' \to 0$, la sucesión $0 \to \operatorname{Hom}_A(M'',E) \to \operatorname{Hom}_A(M,E) \to \operatorname{Hom}_A(M',E) \to 0$ es exacta.

Una caracterización de los módulos inyectivos en términos de los ideales de A es la que proporciona el “Lema de Baer".

Lema. 55.7. (Lema de Baer)
Para un A–módulo E son equivalentes:

(a) E es un A–módulo inyectivo.
(b) Se puede completar cualquier diagrama

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{incl} & A \\ & & \downarrow & \swarrow & \\ & & E & & \end{array}$$

DEMOSTRACIÓN. Consideramos el siguiente diagrama con fila exacta.

$$\begin{array}{ccccc} 0 & \longrightarrow & N & \longrightarrow & M \\ & & f\downarrow & & \\ & & E & & \end{array}$$

La familia $\Gamma = \{(N',f') \mid N \subseteq N' \subseteq M, \text{ y } f' : N' \to E \text{ verifica } f'_{|N} = f\}$ es no vacía, ya que $(N,f) \in \Gamma$. Por otro lado podemos considerar la siguiente relación de orden $(N_1,f_1) \leq (N_2,f_2)$ si $N_1 \subseteq N_2$ y $f_{2|N_1} = f_1$. Podemos probar que cada cadena en Γ tiene una cota superior en Γ, y por el lema de Zorn existe $(N',f') \in \Gamma$ maximal. Para simplificar podemos suponer que $(N',f') = (N,f)$. Si $N = M$, tenemos la extensión buscada. Si $N \neq M$, sea $m \in M \setminus N$. Si $Am \cap N = \{0\}$, entonces $N + Am = A \oplus Am$, y existe una extensión de f definiendo la imagen de m igual a 0; lo que es una contradicción. Si $Am \cap N \neq \{0\}$, consideramos $\mathfrak{a} = (N : m)$, y definimos $g : \mathfrak{a} \to E$ mediante $g(a) = f(am)$. Por la hipótesis, existe una extensión g' de g:

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{incl} & A \\ & & g\downarrow & \swarrow g' & \\ & & E & & \end{array}$$

Definimos $f' : N + Am \to E$ mediante $f'(n + am) = f(n) + ag'(1)$. Tenemos que ver que f' está bien definida; sean $n_1 + a_1 m = n_2 + a_2 m$, entonces $n_1 - n_2 = (a_2 - a_1)m$, luego $f(n_1) - f(n_2) = f(n_1 - n_2) = f((a_2 - a_1)m) = g(a_2 - a_1) = g'(a_2 - a_1) = (a_2 - a_1)g'(1) = a_2 g'(1) - a_1 g'(1)$. Además es claro que f' extiende a f; lo que es una contradicción. □

Un ejemplo típico de módulo inyectivo lo proporciona el cuerpo de fracciones de un dominio.

Proposición. 55.8.
Si D es un dominio con cuerpo de fracciones K entonces K es un D–módulo inyectivo.

DEMOSTRACIÓN. Consideramos el siguiente diagrama:

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathfrak{a} & \xrightarrow{incl} & D \\ & & {\scriptstyle f}\downarrow & & \\ & & K & & \end{array}$$

Para cada $0 \neq a \in \mathfrak{a}$ se tiene $\frac{f(a)}{a} \in K$, y definimos $g : D \to K$ mediante $g(x) = x\frac{f(a)}{a}$. Veamos que g extiende a f. En efecto, si $b \in \mathfrak{a}$, tenemos $g(b) = b\frac{f(a)}{a} = \frac{bf(a)}{a} = \frac{f(ba)}{a} = \frac{f(b)a}{a} = f(b)$. □

Proposición. 55.9.
Sea D un dominio. Dados $\mathfrak{a}, \mathfrak{b} \subseteq D$, $\mathfrak{a} \neq 0$, se tiene de forma natural $(\mathfrak{b} : \mathfrak{a}) \cong \mathrm{Hom}_D(\mathfrak{a}, \mathfrak{b})$.

DEMOSTRACIÓN. Dada la inclusión $f : \mathfrak{a} \hookrightarrow D$, tenemos $\mathrm{Hom}_D(D,K) \xrightarrow{f^*} \mathrm{Hom}_D(\mathfrak{a},K)$, que es sobreyectiva ya que K es un D–módulo inyectivo. Por otro lado $\mathrm{Hom}_D(D,K)$ se identifica con K vía $g \mapsto g(1)$. Como la aplicación f^* está definida $f^*(g) = g \circ f$, para cada $a \in \mathfrak{a}$ tenemos $f^*(g)(a) = (g \circ f)(a) = g(f(a)) = g(1a) = ag(1)$; esto es, $f^*(g)$ es la multiplicación for $g(1)$. Veamos que f^* es inyectiva; si $f^*(g) = 0$, entonces para cada $0 \neq a \in \mathfrak{a}$ se tiene $ag(1) = 0$, y por tanto $g(1) = 0$; esto es $\mathrm{Ker}(f^*) = \{0\}$, y f^* es un isomorfismo.

Por otro lado tenemos $\mathfrak{b} \overset{g}{\hookrightarrow} D \overset{h}{\hookrightarrow} K$, y tenemos homomorfismos $\mathrm{Hom}_D(\mathfrak{a},\mathfrak{b}) \xrightarrow{g_*} \mathrm{Hom}_D(\mathfrak{a},D) \xrightarrow{h_*} \mathrm{Hom}_D(\mathfrak{a},K) \cong K$. Con la identificación anterior se tiene $\mathrm{Hom}_D(\mathfrak{a},\mathfrak{b}) = \{k \in K \mid k\mathfrak{a} \subseteq \mathfrak{b}\} = \mathfrak{b}$.
El ser natural significa que si tenemos homomorfismos $h : \mathfrak{a}' \to \mathfrak{a}$ y $l : \mathfrak{b} \to \mathfrak{b}'$, entonces el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} (\mathfrak{b} : \mathfrak{a}) & \longrightarrow & \mathrm{Hom}_D(\mathfrak{a},\mathfrak{b}) \\ \downarrow & & \downarrow {\scriptstyle h^* \circ l_*} \\ (\mathfrak{b}' : \mathfrak{a}') & \longrightarrow & \mathrm{Hom}_D(\mathfrak{a}',\mathfrak{b}') \end{array}$$

□

Proposición. 55.10.
Sea D un dominio. Para un ideal $0 \neq \mathfrak{a} \subseteq D$ son equivalentes:

(a) $\mathfrak{a}$ es invertible.
(b) $\mathfrak{a}$ es proyectivo.
(c) $\mathfrak{a}$ es proyectivo finitamente generado.

DEMOSTRACIÓN. (a) $\Rightarrow$ (c). Si $\mathfrak{a}$ es invertible, tenemos $\mathfrak{a}(D:\mathfrak{a}) = D$, y por tanto $\mathfrak{a}$ es proyectivo y finitamente generado. Ver Proposición (55.15.).

(c) $\Rightarrow$ (b). Es inmediato.

(b) $\Rightarrow$ (a). Si $\mathfrak{a}$ es proyectivo, existe un homomorfismo sobreyectivo $p : D^{(I)} \rightarrow \mathfrak{a}$ que escinde. Sea $q : \mathfrak{a} \rightarrow D^{(I)}$ tal que $p \circ q = \mathrm{id}_{\mathfrak{a}}$. Llamamos $x_i = p(e_i) \in \mathfrak{a}$.

Para cada índice $i \in I$ tenemos $q_i : \mathfrak{a} \xrightarrow{q} D^{(I)} \xrightarrow{p_i} D$. Observa que $q_i \in \mathrm{Hom}_D(\mathfrak{a}, D = (D:\mathfrak{a}) = \mathfrak{a}^{-1}$. Para cada $a \in \mathfrak{a}$ tenemos $a = p \circ q(a) = p(q(a)) = p(\sum_{i\in I} e_i q_i(a)) = \sum_{i\in I} p(e_i) q_i(a) = \sum_{i\in I} x_i q_i(a) = (\sum_{i\in I} x_i q_i)(a)$. Tenemos entonces $\sum_{i\in I} x_i q_i = 1$ ya que D es un dominio y $\mathfrak{a} \neq 0$. Como consecuencia $\mathfrak{a}$ es un ideal finitamente generado. □

Podemos entonces concluir con el resultado que andábamos buscando.

Teorema. 55.11.
Sea D un dominio. Son equivalentes:

(a) Cada ideal no nulo de D es invertible. (D es un dominio de Dedekind.)
(b) Cada submódulo de un módulo libre finitamente generado es proyectivo.

En particular D es un dominio noetheriano.

DEMOSTRACIÓN. (a) $\Rightarrow$ (b). Si cada ideal no nulo de D es invertible, entonces es proyectivo y finitamente generado, y por inducción tenemos que cada submódulo de un módulo libre finitamente generado es proyectivo finitamente generado.

(b) $\Rightarrow$ (a). Si cada submódulo de D^n es proyectivo, en particular cada submódulo no nulo de D es proyectivo, y por tanto es invertible. □

Ejercicio. 55.12.
Sea D un dominio noetheriano. Prueba que son equivalentes:

(a) D es normal.
(b) Cada sobreanillo fracionario B coincide con D.

SOLUCIÓN. (a) $\Rightarrow$ (b). Si $D \subseteq B \subseteq K$ es un sobreanillo fraccionario, para cada $b \in B$ existe $0 \neq d \in D$ tal que $dD[b] \subseteq D$, y por ser D noetheriano, resulta que es un D–módulo finitamente generado, luego $D[b]$ es un D–módulo finitamente generado y b es entero sobre D, luego $B \subseteq D$.

(b) $\Rightarrow$ (a). Sea $x \in K$ entero sobre D, entonces $D[b]$ es un D–módulo finitamente generado, y por tanto es un sobreanillo fraccionario, luego $D[b] = D$ y $b \in D$. □

Módulos proyectivos sobre anillos locales

Vamos a estudiar anillos a través de sus módulos proyectivos finitamente generados. El primer resultado nos asegurar que ciertos módulos proyectivos finitamente generados son libres.

Teorema. 55.13.
Si A es un anillo local, entonces todo módulo proyectivo finitamente generado es libre.

DEMOSTRACIÓN. Sea M un módulo proyectivo finitamente generado, N otro módulo tal que $M \oplus N \cong A^n$ y $\mathfrak{m} \subseteq A$ el ideal maximal de A. Consideramos los $A/\mathfrak{m}$–módulos $M \otimes (A/\mathfrak{m}) \cong M/\mathfrak{m}M$ y $N \otimes (A/\mathfrak{m}) \cong N/\mathfrak{m}N$. Tenemos que ambos son $A/\mathfrak{m}$–módulos proyectivos, y por tanto libres:

$$(A/\mathfrak{m})^n \cong A^n \otimes_A (A/\mathfrak{m}) \cong (M \oplus N) \otimes_A (A/\mathfrak{m}) \cong (M \otimes_A (A/\mathfrak{m})) \oplus (N \otimes_A (A/\mathfrak{m})) \cong (M/\mathfrak{m}M) \oplus (N/\mathfrak{m}N).$$

Supongamos que $M/\mathfrak{m}M \cong (A/\mathfrak{m})^r$ y $N/\mathfrak{m}N \cong (A/\mathfrak{m})^s$, entonces $r + s = n$.

Dado un sistema de generadores $\{\overline{m_1}, \ldots, \overline{m_r}\}$ de $M/\mathfrak{m}M$ y un sistema de generadores $\{\overline{n}_1, \ldots, \overline{n_s}\}$ de $N/\mathfrak{m}N$, vamos a ver que $\{m_1, \ldots, m_r, n_1, \ldots, n_s\}$ es linealmente independiente en $M \oplus N$, y por tanto $\{m_1, \ldots, m_r\}$ es linealmente independiente, y M será libre de rango r.

Por el isomorfismo $A^n \cong M \oplus N$ tenemos dos sistemas de generadores de A^n: $\{e_1, \ldots, e_n\}$, la base canónica, y $\{x_1, \ldots, x_n\} := \{m_1, \ldots, m_r, n_1, \ldots, n_s\}$. Podemos escribir

$$e_i = \sum_{j=1}^n a_{i,j} x_j \qquad x_j = \sum_{h=1}^n b_{j,h} e_h, \text{ o}$$

$$(e_i)_i = A(x_j)_j \qquad (x_j)_j = B(e_i)_i.$$

Estas últimas expresiones en notación matricial. En consecuencia $(e_i)_i = A(x_j)_j = AB(e_i)$. Como los $\{e_i\}_i$ son una base, se tiene $AB = 1$. Por otro lado se tiene $(x_j)_j = BA(x_j)_j$. Entonces $(BA - 1)(x_j)_j = 0$; tomando clases módulo $\mathfrak{m}$, tenemos $\overline{B}\,\overline{A} - 1 = 0$, por lo tanto $BA - 1 \in M_n(\mathfrak{m}) = M_n(\mathrm{Jac}(A)) = \mathrm{Jac}(M_n(A))$; por la caracterización de los elementos del radical de Jacobson: $\mathrm{Jac}(R) = \{x \in R \mid$ para todo $r \in R$ el elemento $1 - xr$ es invertible a derecha$\}$, se tiene que BA tiene un inverso a la derecha C, que verifica $BAC = 1$. Por tanto B es invertible, y también lo es A. Este último resultado nos dice que $\{x_j\}_j$ es linealmente independiente, tal y como deseábamos. □

Vamos a aplicar este resultado al estudio de un anillo cualquiera.

Al considerar el espectro $\operatorname{Spec}(A)$ de un anillo A, para cada ideal primo $\mathfrak{p} \in \operatorname{Spec}(A)$ el anillo $A_\mathfrak{p}$ es local, y para cada A–módulo proyectivo y finitamente generado M tenemos que $M_\mathfrak{p}$ es un $A_\mathfrak{p}$–módulo proyectivo y finitamente generado, y por tanto libre.

Para cada A–módulo proyectivo finitamente generado M y cada ideal primo $\mathfrak{p}$, se define el **rango** de M en $\mathfrak{p}$ como el rango del $A_\mathfrak{p}$–módulo libre $M_\mathfrak{p}$; lo representamos por $\operatorname{rng}_\mathfrak{p}(M)$. Observa que el rango de M en $\mathfrak{p}$, utilizando que $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ es el cuerpo de fracciones K del dominio de integridad $A/\mathfrak{p}$, se puede calcular como el rango del espacio vectorial sobre K definido a partir de $M/\mathfrak{p}M$.

Tenemos para cada A–módulo proyectivo finitamente generado M una aplicación $\rho_M : \operatorname{Spec}(A) \to \mathbb{N}$ definida por $\rho_M(\mathfrak{p}) = \operatorname{rng}_\mathfrak{p}(M)$.

Proposición. 55.14.
En la situación anterior la aplicación $\rho : \operatorname{Spec}(A) \to \mathbb{N}$ es continua, cuando consideramos en $\mathbb{N}$ la topología discreta: cada punto es abierto.
En particular, si A es un dominio, entonces ρ_M es una aplicación constante.

DEMOSTRACIÓN. Dado $n \in \mathbb{N}$ vamos a ver que $\rho_M^{-1}(n)$ es un subconjunto abierto. Si $\rho_M^{-1}(n) = \varnothing$ es claro que es abierto. Por otro lado, si $\rho_M^{-1}(n) \neq \varnothing$, tomamos $\mathfrak{p} \in \rho_M^{-1}(n)$; vamos a determinar un entorno abierto de $\mathfrak{p}$ contenido en $\rho_M^{-1}(n)$.
Tenemos $\operatorname{rng}_\mathfrak{p}(M) = n$, esto es, $\operatorname{rng}(M_\mathfrak{p}) = n$ (como $A_\mathfrak{p}$–módulo). Sean $x_1, \ldots, x_n \in M$ tales que $\{x_1/1, \ldots, x_n/1\}$ es una base de $M_\mathfrak{p}$.
Definimos $f : A^n \to M$ mediante $f(e_i) = x_i$, para $i = 1, \ldots, n$. Podemos entonces escribir la siguiente sucesión con filas exactas:

$$0 \longrightarrow H := \operatorname{Ker}(f) \longrightarrow A^n \xrightarrow{\ f\ } M \longrightarrow L := \frac{M}{\operatorname{Im}(f)} \longrightarrow 0$$

$$A^n \searrow \operatorname{Im}(f) \nearrow M, \qquad 0 \nearrow \operatorname{Im}(f) \searrow 0$$

Tenemos que $f_\mathfrak{p}$ es un isomorfismo, luego la sucesión siguiente es exacta:

$$0 \longrightarrow H_\mathfrak{p} \longrightarrow A_\mathfrak{p}^n \xrightarrow[\cong]{\ f_\mathfrak{p}\ } M_\mathfrak{p} \longrightarrow L_\mathfrak{p} \longrightarrow 0$$

En particular $L_\mathfrak{p} = 0$. Como L es un A–módulo finitamente generado, existe $s \in A \setminus \mathfrak{p}$ tal que $sL = 0$; por lo tanto, al considerar la localización en $\Sigma = \{1, s, s^2, \ldots\}$, tenemos $L_s = 0$, y por lo tanto una sucesión exacta

$$0 \longrightarrow H_s \longrightarrow A_s^n \xrightarrow{\ f_s\ } M_s \longrightarrow 0$$

Ésta es una sucesión de A_s–módulos, y M_s es proyectivo como A_s–módulo, por lo tanto esta sucesión escinde, y H_s es un A_s–módulo finitamente generado. Podemos localizar en $\mathfrak{p}$ (ó en $\mathfrak{p}A_s$), verificándose $(M_s)_\mathfrak{p} = M_\mathfrak{p}$, e igual para los demás. Tenemos entonces una sucesión exacta corta:

$$0 \longrightarrow H_\mathfrak{p} \longrightarrow A^n_\mathfrak{p} \xrightarrow[\cong]{f_\mathfrak{p}} M_\mathfrak{p} \longrightarrow 0$$

y como H_s es finitamente generado, existe $t/1 \in A_s \setminus \mathfrak{p}A_s$, esto es, $t \in A \setminus \mathfrak{p}$, tal que $tH_s = 0$. Al considerar el conjunto multiplicativo $\Sigma = \{1, st, (st)^2, \ldots\} \subseteq A$ tenemos una sucesión exacta

$$0 \longrightarrow H_{st} = 0 \longrightarrow A^n_{st} \xrightarrow{f_{st}} M_{st} \longrightarrow L_{st} = 0 \longrightarrow 0$$

y por tanto f_{st} es un isomorfismo y tenemos $f_{st} : A^n_{st} \cong M_{st}$.
Dado $\mathfrak{q} \in \operatorname{Spec}(A)$ tal que $st \notin \mathfrak{q}$, para cada A–módulo N se tiene $N_\mathfrak{q} = (N_{st})_\mathfrak{q}$, y por lo tanto $f_\mathfrak{q} : A^n_\mathfrak{q} \cong M_\mathfrak{q}$, luego $\mathcal{X}(st) = \{\mathfrak{q} \in \operatorname{Spec}(A) \mid st \notin \mathfrak{q}\}$ es un entorno abierto de $\mathfrak{p}$ contenido en $\rho_M(n)$, y éste es un conjunto abierto.
Si suponemos que A es un dominio, entonces $0 \in \operatorname{Spec}(A)$, y para cada ideal primo $\mathfrak{p}$ se tiene $0 \subseteq \mathfrak{p}$. Si $s \notin \mathfrak{p}$, entonces $s \notin 0$, luego 0 pertenece a cada abierto de $\mathfrak{p}$, por lo tanto $\rho_M(0) = \rho_M(\mathfrak{p})$, y ρ_M es una aplicación constante. □

Ideales fraccionarios proyectivos

Proposición. 55.15.
Sea D un dominio y $\mathfrak{a}$ un ideal fraccionario. Si $\mathfrak{a}$ es invertible, entonces $\mathfrak{a}$ es proyectivo finitamente generado.

DEMOSTRACIÓN. Si $\mathfrak{a}\mathfrak{a}^{-1} = D$, existen $x_1, \ldots, x_n \in \mathfrak{a}$ e $y_1, \ldots, y_n \in \mathfrak{a}^{-1}$ tales que $1 = \sum_{i=1}^n x_i y_i$. Para cada $a \in \mathfrak{a}$ se tiene $a = a\sum_{i=1}^n x_i y_i = \sum_{i=1}^n x_i(ay_i)$, luego $\{x_1, \ldots, x_n\}$ es un sistema de generadores de $\mathfrak{a}$. Para ver que es proyectivo, consideramos el homomorfismo $f : A^n \to \mathfrak{a}$ definido por $f(e_i) = x_i$, para $i = 1, \ldots, n$; veamos que tiene un inverso a la derecha. Definimos $g : \mathfrak{a} \to A^n$ mediante $g(a) = (ay_1, \ldots, ay_n) \in A^n$. Es claro que $f \circ g = \mathrm{id}_\mathfrak{a}$, y por tanto $\mathfrak{a}$ es un sumando directo de A^n. □

Proposición. 55.16.
Si D es un dominio de Dedekind, el grupo de clases $\operatorname{Cl}(D) = \mathcal{F}(D)/\mathcal{P}(D)$ es isomorfo al grupo de clases de isomorfía de ideales fraccionarios.

DEMOSTRACIÓN. Por ser D un dominio de Dedekind tenemos que $\mathcal{F}(D)$ es un grupo. Sean $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(D)$ tales que existe un isomorfismo $f : \mathfrak{a} \cong \mathfrak{b}$; fijado $0 \neq x \in \mathfrak{a}$, para cada $a \in \mathfrak{a}$ tenemos $f(xa) =$

$xf(a) = af(x)$. Por ser f un isomorfismo se tiene $x\mathfrak{b} = \mathfrak{a}f(x)$, entonces $\mathfrak{b} = \frac{f(x)}{x}\mathfrak{a}$. El recíproco también es cierto, y por tanto para $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(D)$ se tiene $\mathfrak{a} \cong \mathfrak{b}$ si, y sólo si, $\mathfrak{a}\mathcal{P}(D) = \mathfrak{b}\mathcal{P}(D)$. □

Proposición. 55.17.
Si D es un dominio de Dedekind, cada módulo proyectivo finitamente generado es isomorfo a una suma directa de ideales de D.

DEMOSTRACIÓN. Dado P, un módulo proyectivo finitamente generado, tomamos $n \in \mathbb{N}$ tal que $M \hookrightarrow D^n$. Si $n = 1$, entonces P es isomorfo a un ideal de D. Supongamos que el resultado es cierto para $m < n$, y vamos a estudiar el caso n. Consideramos la proyección $D^n \xrightarrow{p} D$. Si $p(P) = 0$, entonces $P \hookrightarrow D^{n-1}$, y el resultado es cierto. Si $p(P) \neq 0$, tenemos el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & D^{n-1} \cap P & \longrightarrow & P & \longrightarrow & p(P) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & D^{n-1} & \longrightarrow & D^n & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

Por ser D un dominio de Dedekind todo ideal fraccionario es proyectivo, en particular $p(P)$ es proyectivo y la sucesión de la fila superior escinde, esto es, $P \cong (D^{n-1} \cap P) \oplus p(P)$, en donde cada sumando es isomorfo a una suma directa de ideales de D. □

Existe una expresión más sencilla para los módulos proyectivos finitamente generados sobre un dominio de Dedekind que vamos a tratar de justificar.

Lema. 55.18.
Sea D un dominio de Dedekind, $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}(D)$ tales que $\mathfrak{b} \subseteq D$, existe $a \in \mathfrak{a}$ tal que $a\mathfrak{a}^{-1} + \mathfrak{b} = D$.

DEMOSTRACIÓN. Supongamos que $\mathfrak{b} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$. Consideramos $a_i \in \mathfrak{a}\mathfrak{p}_1 \cdots \widetilde{\mathfrak{p}_i} \cdots \mathfrak{p}_t \setminus \mathfrak{a}\mathfrak{p}_1 \cdots \mathfrak{p}_t$. Se tiene $a_i\mathfrak{a}^{-1} \in \mathfrak{p}_1 \cdots \widetilde{\mathfrak{p}_i} \cdots \mathfrak{p}_t \setminus \mathfrak{p}_1 \cdots \mathfrak{p}_t$, y por lo tanto, si llamamos $a = a_1 + \cdots + a_t$, se tiene $a\mathfrak{a}^{-1} \notin \mathfrak{p}_i$, para $i = 1, \ldots, t$. Como consecuencia $a\mathfrak{a}^{-1} + \mathfrak{b} = D$, ya que son comaximales por no tener primo en común. □

Corolario. 55.19.
Sea D un dominio de Dedekind y $\mathfrak{a}_1, \mathfrak{a}_2 \in \mathcal{F}(D)$, se tiene $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \cong D \oplus \mathfrak{a}_1\mathfrak{a}_2$.

DEMOSTRACIÓN. Dado $0 \neq a_1 \in \mathfrak{a}_1$, tenemos $a_1\mathfrak{a}_1^{-1} \subseteq D$, entonces existe $a_2 \in \mathfrak{a}_2$ tal que $a_2\mathfrak{a}_2^{-1} + a_1\mathfrak{a}_1^{-1} = D$. Podemos encontrar $b_i \in \mathfrak{a}_i^{-1}$ tales que $a_1b_1 + a_2b_2 = 1$. En consecuencia es cierto que

$$\begin{pmatrix} b_1 & b_2 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} a_1 & -b_2 \\ a_2 & b_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

y podemos definir una aplicación $\mathfrak{a}_1 \oplus \mathfrak{a}_2 \longrightarrow D \oplus \mathfrak{a}_1\mathfrak{a}_2$ mediante

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} b_1 & b_2 \\ -a_2 & a_1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Como la matriz que define esta aplicación es invertible, tenemos un isomorfismo. □

Corolario. 55.20.
Sea D un dominio de Dedekind. Para cada módulo proyectivo finitamente generado P de rango n existe un ideal $\mathfrak{a} \subseteq D$ tal que $P \cong D^{n-1} \oplus \mathfrak{a}$.
Si P_1 y P_2 son módulos proyectivos de rangos n_1 y n_2, respectivamente, y $P_i \cong D^{n_i-1} \oplus \mathfrak{a}_i$, para $i = 1, 2$, entonces $P_1 \oplus P_2 \cong D^{n_1+n_2-1} \oplus \mathfrak{a}_1\mathfrak{a}_2$.

Observa que este resultado pone de manifiesto que existe una relación entre el producto de ideales y la suma directa de módulos proyectivos finitamente generados.

Este resultado se extenderá, para tener en cuenta las estructuras algebraicas subyacentes, al considerar clases de isomorfía de módulos proyectivos finitamente generados y un grupo definido a partir de las mismas; de esta forma obtendremos un grupo isomorfo al grupo de clases del dominio de Dedekind D.

56. Ejercicios

Dominios de valoración discreta

Ejercicio. 56.1.
Sea A un dominio de valoración discreta con ideal maximal $\mathfrak{m}$ y cuerpo residual $F = A/\mathfrak{m}$. Demuestra que para todo entero natural n el F–espacio vectorial $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ es de dimensión uno.

SOLUCIÓN

Ejercicio. 56.2.
Sea A un dominio de integridad local con ideal maximal $\mathfrak{m} = (t) \neq 0$. Si $\cap_{n\geq 1}(t^n) = 0$, demuestra que A es un dominio de valoración discreta.

SOLUCIÓN

Ejercicio. 56.3.
Sea A un anillo local noetheriano con ideal maximal $\mathfrak{m} = (t)$. Demuestra que se verifica una de las dos posibilidades:

(1) A es un dominio de valoración discreta o
(2) existe un entero natural n tal que $t^n = 0$.

En el último caso demuestra que A es artiniano.

SOLUCIÓN

Ejercicio. 56.4.
Sea A un dominio de integridad noetheriano local con ideal maximal $\mathfrak{m} \neq 0$ y cuerpo residual $F = A/\mathfrak{m}$.

(1) Demuestra $\mathfrak{m}/\mathfrak{m}^2$ es un espacio vectorial sobre F.
(2) Demuestra que si $\dim_F(\mathfrak{m}/\mathfrak{m}^2) = 1$, entonces A es un dominio de valoración discreta.
(3) Si todo ideal no nulo de A es una potencia de $\mathfrak{m}$, demuestra que A es un dominio de valoración discreta.

SOLUCIÓN

Ejercicio. 56.5.
Sea D un dominio de valoración discreta con cuerpo de fracciones K y E un anillo intermedio. Prueba que son equivalentes:

(a) E es un dominio de valoración discreta.
(b) $E = D$.

SOLUCIÓN

Ejercicio. 56.6.
Sea A un dominio de integridad noetheriano local con ideal maximal $\mathfrak{m} \neq 0$. Prueba que son equivalentes:

(a) A es un anillo de valoración discreta;
(b) los únicos ideales primarios (no nulos) de A son las potencias de $\mathfrak{m}$.

SOLUCIÓN

Ideales fraccionarios

Ejercicio. 56.7.
Sea A un dominio de integridad con cuerpo de fracciones K.

(1) Prueba que todo A-submódulo no nulo finitamente generado de K es un ideal fraccionario de A.
(2) Si A es un dominio noetheriano, prueba que $\mathfrak{a}$ es un ideal fraccionario de A si, y sólo si, $\mathfrak{a} \subseteq K$ es un A-submódulo finitamente generado.

SOLUCIÓN

Ejercicio. 56.8.
Sea A un dominio de integridad. Demuestra que todo ideal fraccionario de A es invertible si y sólo si todo ideal entero de A es invertible.

SOLUCIÓN

Ejercicio. 56.9.
Sea A un dominio de integridad y $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales fraccionarios de A tales que su producto es un ideal fraccionario principal: $\mathfrak{a}_1 \cdots \mathfrak{a}_n = aA$.Demuestra que todos los ideales $\mathfrak{a}_i$ son invertibles.

SOLUCIÓN

Ejercicio. 56.10.
Sea A un dominio de integridad con cuerpo de fracciones K y $\mathfrak{p}$ un ideal primo no nulo de A. Demuestra que los ideales fraccionarios de $A_\mathfrak{p}$ son exactamente los $A_\mathfrak{p}$–submódulos de K de la forma $\mathfrak{a}A_\mathfrak{p}$, con $\mathfrak{a}$ un ideal fraccionario de A.

SOLUCIÓN

Dominios de Dedekind

Ejercicio. 56.11.
Sea A un dominio de Dedekind. Demuestra que para todo subconjunto multiplicativo Σ de A el anillo de fracciones $\Sigma^{-1}A$ es un cuerpo o es un dominio de Dedekind.

SOLUCIÓN

Ejercicio. 56.12.
Sean $\mathfrak{a}, \mathfrak{b}$ ideales fraccionarios de un dominio de Dedekind A y n un entero no nulo. Demuestra que $\mathfrak{a}^n = \mathfrak{b}^n$ si y sólo si $\mathfrak{a} = \mathfrak{b}$.

SOLUCIÓN

Ejercicio. 56.13.
Sea A un dominio de integridad noetheriano que no es un cuerpo. Prueba que son equivalentes:
(a) A es un dominio de Dedekind;
(b) $A_\mathfrak{m}$ es un anillo de valoración discreta para todo ideal maximal $\mathfrak{m}$.

SOLUCIÓN

Ejercicio. 56.14.
Sea A un dominio noetheriano que no es un cuerpo. Prueba que son equivalentes:
(a) A es un dominio de Dedekind;
(b) para todo ideal maximal $\mathfrak{m}$ de A no existe ningún ideal $\mathfrak{a}$ tal que $\mathfrak{m}^2 \subsetneq \mathfrak{a} \subsetneq \mathfrak{m}$.

SOLUCIÓN

Ejercicio. 56.15.
Sea A un dominio noetheriano que no es un cuerpo. Prueba que son equivalentes;

(a) *A es un dominio de Dedekind;*
(b) *todo ideal primo no nulo de A es maximal y todo ideal $\mathfrak{p}$–primario es una potencia de $\mathfrak{p}$.*

SOLUCIÓN

Ejercicio. 56.16.
Sea D un dominio de Dedekind. Prueba que se verifica:

(1) *Cada elemento no nulo $a \in D$ está contenido en sólo un número finito de ideales maximales.*
(2) *Si $\mathfrak{a} \subseteq \mathfrak{b} \subseteq D$, existe un ideal $\mathfrak{c} \subseteq D$ tal que $\mathfrak{a} = \mathfrak{c}\mathfrak{b}$.*

SOLUCIÓN

Ejercicio. 56.17.
Sea D un dominio semilocal, cada ideal invertible es principal.

SOLUCIÓN

Ejercicio. 56.18.
Un dominio de Dedekind D que tiene sólo un número finito de ideales maximales es un DIP.

SOLUCIÓN

Ejercicios del capítulo

Ejercicio. 56.19.
Razonar sobre la veracidad o falsedad de las siguientes afirmaciones:

(1) *Todo dominio de Dedekind es un dominio de ideales principales.*
(2) *Sea D un dominio de integridad. Todo ideal fraccionario de D es invertible si, y solo si, todo ideal entero de D es invertible.*
(3) *Sea D un dominio de Dedekind, $\mathfrak{a}, \mathfrak{b}$ ideales fraccionarios y n un entero no nulo.Se tiene $\mathfrak{a}^n = \mathfrak{b}^n$ si, y solo si, $\mathfrak{a} = \mathfrak{b}$.*

(4) *Sea* $\mathfrak{p}$ *un ideal primo de* A. *Si* $\mathfrak{a}_\mathfrak{p}$ *es el núcleo del homomorfismo* $A \to A_\mathfrak{p}$, *entonces* $\mathfrak{a}_\mathfrak{p} \subseteq \mathfrak{p}$.
(5) *Si* $\mathfrak{a} \subseteq A$ *es un ideal nilpotente, entonces* $\dim(A) = \dim(A/\mathfrak{a})$.
(6) $\dim(A) = \sup\{\dim(A_\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Spec}(A)\}$.
(7) *Sea* D *un dominio de integridad y* $\Sigma \subseteq D$ *un subconjunto multiplicativo, entonces* $\Sigma^{-1}D$ *es un subanillo del cuerpo de fracciones de* D.
(8) *Sea* D *un dominio de ideales principales y* $\Sigma \subseteq D$ *un subconjunto multiplicativo, entonces* $\Sigma^{-1}D$ *es un dominio de ideales principales.*
(9) $A \subseteq B$ *es una extensión entera de anillos en la que todo ideal primo no nulo de* A *es maximal, entonces todo ideal primo no nulo de* B *es maximal.*
(10) *Si* $A \subseteq B$ *una extensión entera de anillos y* $u_1, \ldots, u_t \in B$ *son elementos enteros sobre* A, *entonces* $A[u_1, \ldots, u_t]$ *es un* A-*módulo finitamente generado.*
(11) *En un anillo artiniano* A, $\operatorname{Nil}(A) \neq \operatorname{Jac}(A)$.

SOLUCIÓN

Bibliografía

[1] W. W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, Graduate Studies in Mathematics, 3, American Mathematical Society, 1994.

[2] M. F. Atiyah and I. G. Macdonald, *Introducción al álgebra conmutativa*, Reverté, Barcelona, 1973.

[3] Celine Carstensen, Benjamin Fine, and Rosenberger, *Abstract algebra. applications to galois theory, algebraic geometry and cryptography*, De Gruyter, 2011.

[4] I. S. Cohen, *Rings with restricted minimum condition*, Duke Math. J. **17** (1950), 27–42. 28.11.

[5] P. M. Cohn, *Basic algebra*, Springer, 2003.

[6] D. Cox, J. J. Little, and D. O'Shea, *Ideals, varieties and algorithms*, Undergraduate Texts in Math., Springer–Verlag, 1992.

[7] R. M. Dummitn, D. S. ; Foote, *Abstract algebra. 3rd ed.*, Wiley, 2004.

[8] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate texts in mathematics, 150, Springer–Verlag, 1995.

[9] N. Jacobson, *Basic algebra II. 2nd ed.*, Freeman, 1989.

[10] G. J. Janusz, *Algebraic number theory*, Academic Press, 1973.

[11] I. Kaplansky, *Commutative rings*, Chicago Univ. Press, 1974. 8.41., 8.42., 8.43.

[12] E. Kunz, *Introduction to commutative algebra and algebraic geometry (segunda edición corregida)*, Birkhauser, 1991.

[13] S. Lang, *Algebra 3rd. ed.*, Springer, 2002.

[14] H. Matsumura, *Commutative algebra*, Benjamin, 1980.

[15] N. Nagata, *Local rings*, R. E. Krieger Publ. Co., 1975.

[16] M. Reid, *Undergraduate commutative algebra*, London Math. Soc. Student Texts, 29, Cambridge Univ. Press, 1995.

[17] J. J. Watkins, *Topics in commutative algebra*, Princeton University Press, 2007.

Índice alfabético